CHAPTER 5

Information Systems Management

Introduction

Today's world is complex. Organizational environment is becoming increasingly complicated with the integration of various technologies to provide better business delivery. While one's need of effective and efficient delivery is fulfilled through the means of new technologies, such as internet, video, audio, business presentations, and business meetings, interplaying with each other, the other need requires more focus and strengthening, that is, information security. Businesses have to protect the confidentiality, and the integrity of business information while making their systems available for continued business. A few minutes of down time of an e-commerce business site can lead to a significant amount of missed business or switching over of the business to a competitive supplier. A breach of confidentiality or integrity can lead to reputation loss, huge penalties, or significant revenue loss. To ensure information security, we need to act proactively.

When pro-activeness does not stop the breaches, we need to react effectively and efficiently and when breaches cannot be avoided we need to recover the businesses as fast as possible to provide continued services to the customers. Risk Management when applied in the right spirit, with the deployment of the right methodology, with the involvement of the right people, with the application of the right thinking, and with the execution of the actions effectively, can provide a reasonably good proactive approach to ensure that there is a high chance of avoiding information security breaches or incidents. In spite of being proactive, we cannot be assured that the security breaches cannot happen, as this evolving world provides a lot of opportunities and ways to breach the system. Incident response provides a reactive method to ensure that the breaches are handled, contained, and recovered from effectively. In spite of effective risk management and incident response systems in place, you cannot still be assured of continuity of business or speedy recovery when the organization is affected by severe security breaches or disasters. Hence the need for effective disaster recovery and business continuity systems to be put in place which is again a proactive as well as a reactive system to ensure that the business can still continue in spite of disasters or severe security incidents when there is high probability of speedy recovery. Most of the businesses may go out of business or may lose a significant number of customers if they are not able to recover within a reasonable time frame. Similarly, some of the businesses cannot sustain a short period of lack of availability of systems as some of their business is highly critical and needs to be continued at any cost even at a reduced level of activity / volume.

An effective risk management approach supported by an effective and efficient incident response, supported by an effective and efficient disaster recovery and business continuity system can ensure that the businesses are able to sustain and provide continued services to their clients in spite of serious security breaches or disasters.

Unfortunately, there are hundreds of theories proposed by the experts and varied practices employed by various organizations with respect to risk management, incident response, disaster recovery, and business continuity. The definition of each of these words, from incident to disaster to recovery to continuity varies from theory to theory. In order not to confuse our readers with too many theories and too many definitions we are providing here simple definitions in simple terms with respect to each of these as well as a simple and practical way of handling each of these, which in our view is suitable to most of the organizations in this world. Further, each of the aspects like Risk Management, Incident Response, and Business Continuity Planning can be strongly supported or advocated through

a policy driving the same with clear commitment from top management. However, as we have seen, such policies are merely put in place either because of the requirement of a standard or because of some customer insistence without much thinking and most of the time not revisited for years and are not referred to by the organizational personnel and losing the requisite sanctity. Hence, we have not focused in this chapter much on the policies except with regard to Incident Response Policy which we have included here as guidance.

Risk

Risk is the chance of something adverse happening which has negative consequences on the organization and in the context of this book on information security.

Incident

Any event of consequence to the organization where the organization faces potential loss or is exposed to potential loss can be considered as an incident. Loss can be monetary, business, reputation or loss of customers.

Disaster

Any grave situation which brings down the business partially or fully and which is of serious consequence to the organization can be considered as a disaster. These often may be on account of natural disasters but sometimes these may be on account of manmade activities like terrorism or at other times, they can be on account of severe security incidents like a severe infection of malware crashing all the critical servers. In a way, disasters can be considered more severe than an incident.

Disaster Recovery

Businesses are ongoing and they are meant to be ongoing or continuous entities. Businesses have competitors who always want to take away others' customers or the market share. Businesses hence have to recover their businesses from each disaster speedily so that they are able to service their customers effectively before they plan to switch over to the competitor. Even though disaster recovery can mean any recovery from any disaster, many times it is referred to in the parlance of recovery of IT infrastructure and systems, which in today's context performs a lead role in any business.

Business Continuity

All businesses are ongoing entities. It may be acceptable for a business which is non-critical to its customers to be shut down for a few days but a critical business like banking, health care, telecommunications, e-commerce, and others cannot be shut down for more than a few minutes to more than a few days depending on the business. Hence, they need to continue to sustain the continuity of the critical business may be at a lower scale or volume than the normal scale or volume. Business continuity assures that the plans and systems are in place to continue the business in spite of incidents or disasters. Business continuity includes business recovery post any disaster and is one of the important components as the speed at which you recover from downtime or disruption or disaster and continue business is critical for the success of any organization.

Risk Management

Risk is the chance that something can go wrong or of an adverse event taking place. In the context of information security, risk is something which can impact the availability, confidentiality, or integrity of business or personnel information. Examples of some of the common risks include: laptops being stolen and the data on them being stolen, a person tail gating somebody stealing some critical files, or a person who got the credentials through social engineering means gaining access to the server and copying confidential data, or somebody tapping into the network and modifying the messages being sent, or somebody physically stoning or ransacking the building during a riot, or that of natural hazards like floods. Threats are the risks. Risks need to be proactively managed.

There are various methodologies to carry out risk assessments by the organization. Organizations are also free to come up with their own risk assessment methodologies depending upon their context and their experience. We are exploring one such methodology that is easy to use and practical and has been effectively used for some time.

First, risks need to be identified. Then they need to be analyzed for the probability of their occurrence and the impact if they do happen. Based on the probability of their occurrence and the impact if they happen, the risk exposure or risk level has to be decided. Depending upon the risk exposure of the organization to any particular risk, the risk has to be either avoided, transferred, mitigated, or accepted. Risk can be accepted only when the organization is exposed to minimal risk that it can sustain. Where the risks are decided to be mitigated, additional controls to mitigate them have to be determined. It is normally necessary at this point to determine the additional controls, but it is also extremely important to ensure that these controls are effectively deployed and their continued effectiveness is monitored and ensured. Organizational internal and external context may vary from time to time, maybe due to a competitor environment or due to legal changes or may be due to the way the business is done or else due to the technological changes.

The risks in the revised context need to be analyzed and additional controls need to be implemented as required to ensure that the organization continues to drive sufficient controls to protect information security. It is recommended that each organization has its own clearly defined risk assessment methodology which drives the risk assessment in the organization. This should cover the entire process of risk assessment including the acceptable risk exposure value and guidelines on various risk responses. Figure 5-1 illustrates the risk assessment life cycle.

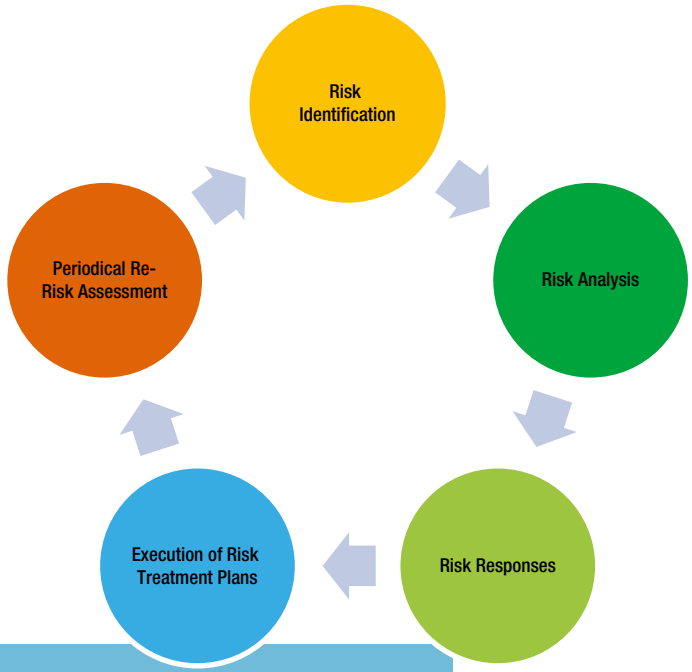

Figure 5-1. *Risk Assessment Life Cycle*

Again, we have seen some organizations using the asset value to calculate the total financial impact. We have seen this approach failing mostly because of lack of accurate asset value. Further, some organizations also try to assess the business impact of the risks in financial terms. Again, as we have seen, it turns out to be mostly guess work rather than based on uniform, good, prudent ways.

In view of the preceding information, we have provided a simple, practical way that works for most of the organizations, which at the same time uses best in class practices from various guidelines and standards including from ISO/IEC 27001:2013 – Information Security Management System – Requirements.

Identification of Risk

The first step to identify the risks in the context of information security is to identify all the information assets of the organization. Information assets include the infrastructure, facilities, hardware, software, applications, utilities and tools, data, employees, contractors, and suppliers which are needed to run any business.

Table 5-1 lists typical information assets that are found in organizations.

Table 5-1. *Typical Information Assets*

Function	Information Asset
Human Resources	Employee Personal Records (with PII); Other Employee Records (Offer Letters, CVs, Offer Letters, Certificates, Performance Appraisal, etc.); Human Resources Management System; Employees (may be further categorized based on type of employees); Suppliers/Third Party Vendors; Recruitment Test Papers and Answer Keys; etc.
Training	Training Material; Training Quiz/Test Papers; Training Feedback and Analysis; Online Tools used for the Training; etc.
Marketing & Sales	Proposals; Marketing Strategies, Marketing Plans; Communications with the Customers including on the scope of new projects, pricing, etc.; Visit Plans of the departmental personnel; etc.
Project Management & Project Teams (including Product Development Teams / Engineering Teams)	Proposals; Communications with the Customers; Customer Provided Property such as Hardware; Customer Provided Information/Data; Project Artifacts; Applications; Utilities; Open Source Software; Third Party Software; Software Code Developed; New Concepts/Innovations yet to be patented; New Processes Invented; Design Documents, Architecture Documents; etc.
Information Technology	Desktops/Workstations; Laptops; Servers; Printers; Communication Equipment; CD/DVD Writers/Tape Drive; Backup Tapes; Scanners; External Hard-disks/USB Pen Drives; Original Licenses/License Keys; Network Cabling; Firewall, Router & Log Analyzer; ISP/External Connectivity; Physical Keys; Specific Servers like Anti-Virus Servers, Application Servers, Database Servers, Patch Management Server, FTP Server etc.; Other utilities used like Remote Connectivity Tools, Monitoring Tools, etc.; Logs of various servers/applications, system administrator activity logs; Encryption Keys; Root and other Administrative logins and passwords; etc.

(*continued*)

Table 5-1. (*continued*)

Function	Information Asset
Finance & Legal	Vendor Agreements/Contracts; Financial/Banking Details/Records; Statutory Records including Notices received, Cases Pending, etc.; Financial Instruments; Payroll, Tax and such other details; Digital Signatures; Login Ids and Passwords of Authorized Persons authorized to carry out different types of tasks on tools like SAP, Oracle Financials, etc.; Compliance Filings; Various reports filed with various statutory and regulatory agencies, etc.
Quality	Process Documents; Quality Records including Audit Records, Management Review Records and other records; Testing Records; Defect Details; Best Known Methods; etc.

Note: a) The functions mentioned are only sample functions and the organizations may have more functions than the above or may be differently organized; b) Some of the above assets may be again bucketed into common, specific depending upon the differential risks e.g. management laptops have different risks compared to the clerical laptops; Customer-provided data like Patient Details, Credit Card details have different risks than the data without much sensitivity like generic data like details of the machines on the shop floor, etc., c) Again, the records / documents may be classified as hard copy records / documents or soft copy records / documents as they carry different risks; d) Tools / Utilities may have to be classified separately depending upon the purpose and their capability; etc.; e) Above list is not comprehensive. It is only illustrative. There may be hundreds of other documents / records / tools / utilities etc. which may be included which may also differ from organization to organization.

The second step is to identify the threats the organization is exposed to with respect to each function within the organization. This may be done based on the historical data with the organization; or data obtained from the local and / or regional and / or national and / or international agencies or institutes of relevance or other sources of learned and reliable information. Additionally, expertise of the organizational employees, contractors, and suppliers is used. Another way is to identify the vulnerabilities the organization is exposed to like tail gating, lack of effective policies, lack of awareness / knowledge, technical vulnerabilities like security flaws in the utilities or applications used, the organization location, and so on, and then identify the threats which may exploit these vulnerabilities. Another way is to identify the threats first and then identify the vulnerabilities which may lead to such threats. However, it is necessary to identify various pairs of threats and vulnerabilities an information asset is exposed to. Each information asset may be exposed to different vulnerabilities which may lead to different threats or each threat may be due to different vulnerabilities. Also, different vulnerabilities may sometimes lead to the same threat. For example, a fire threat may result from storing old paper records and inflammable material in the organization, the kitchen being allowed to use electric or gas stoves, or weak wiring.

A vulnerability of not having adequate awareness of policies may allow some non-employee to tail gate an employee which can lead the stranger to steal confidential files or papers, destroying the data center by planting a bomb, firing at the employees, or killing the employees. This makes clear the need for identifying different sets of vulnerabilities and threats.

Some of the typical pairs of threats and vulnerabilities are listed in Table 5-2.

Table 5-2. *Threats and Vulnerabilities*

Threat	Vulnerability
Malicious Destruction	Lack of Physical Security
Theft and Fraud	Lack of Physical Security
Fire	Lack of Environmental Protection
Flood	Lack of Environmental Protection
Misplace / Loss of Documents	Inadequate Document / File Handling Procedures
Malicious Destruction	Incorrect Access Rights
Theft and Fraud	Incorrect Access Rights
Data Corruption & Loss of Data	Lack of Backups
Theft and Fraud	Access of Production Data to Application Maintenance Engineers
Theft and Fraud	Lack of effective software change management leading to unauthorized changes
Theft and Fraud	Lack of Segregation of Duties
Misuse of Equipment and Facilities	Inconsistent Compliance with Security Policies
Access of Facilities / Systems / Applications / Data by Ex-Employee or others and Possible Thefts and Frauds	Lack of Proper Exit Procedures
Technical Vulnerability	Inadequate Configuration
Undesirable Impact	Inadequate Patch Validation
Malicious Software Infection	Lack of Adequate Monitoring Mechanisms
Malicious Software Infection	Technical Incompatibility
Prey to Social Engineering Tricks	Inadequate Security Awareness & Training
Misuse of credentials	Infrequent change of passwords / Weak Passwords
Technical Failures	Improper / Inappropriate Maintenance
Intrusion / Unauthorized Data Access	Inadequate Firewall / Router Policies
Single Point of Failure	Lack of Redundancy
Service Deficiency	Choice of Wrong Service Provider

Note: a) Above list is only illustrative. It is impossible to cover all threats and vulnerabilities; b) The Threats and Vulnerability applicability depends upon the Information Asset.

The third step is to identify each information asset, the pair of threat and vulnerability, the impact on each of the aspects of information security, that is, confidentiality, integrity, and availability. This can be a rating provided to each information asset, for each pair of threat and vulnerability, in terms of the impact on each of the information security aspects (confidentiality, integrity and availability) that can be compromised or breached. Table 5-3 describes the potential impact on security objectives.[1]

Table 5-3. *Levels of Impact on Security Objectives*[1]

Security Objective	Low Impact	Medium Impact	High Impact
Confidentiality	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Availability	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Amplification	A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in organizational capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.	A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in organizational capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.	A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of organizational capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Low impact on any security objective is given a value of 1, medium impact on any security objective is given a value of 2 and high impact on any security objective is given a value of 3. If any security objective is not applicable to the information asset under consideration then it is given a value of 0. For each information asset, for each pair of threat and vulnerability, the impact value for confidentiality plus the impact value for the integrity plus the impact value for availability gives the total asset impact value. Asset impact is optionally categorized as C1, C2, C3 based on the following total asset impact values listed in Table 5-4.

Table 5-4. *Asset Category Classification Based on Asset Impact Value*

Asset Impact Category	Total Asset Impact Value
C1 – High impact asset	Total Asset Impact Value of 7 or 8 or 9
C2 – Medium impact asset	Total Asset Impact Value of 4 or 5 or 6
C3 – Low impact asset	Total Asset Impact Value of 1 or 2 or 3

The fourth step is to identify the controls already implemented by the organization to manage this risk. These controls may be physical security like security guards; awareness sessions wherein the employees are made aware of the do's and don'ts or specific steps to be taken to avoid, control, and mitigate the risks; or implementation of a tool in the organization like a firewall that eliminates such a risk.

Risk Analysis

Risk analysis is the next important step. At the end of the risk analysis we need to quantify the risk in terms of quantified risk exposure. This is different from the impact levels on confidentiality, integrity, and availability we discussed in the earlier paragraphs.

For a particular information asset, for each of the pair of threat and vulnerability, we identify the actual impact on the business. For example, a banking server compromised and misused may impact the entire business severely, including potential loss of customer confidence, reputation loss, loss of data integrity, or monetary loss. Then we determine the probability of this risk (also known as the likelihood of risk), as shown in Table 5-5. Probability of the rating is from 1% to 99%. A probability of 100% means that the risk is already true and has already occurred.

Table 5-5. *Risk Probability Ratings*

Probability	Description	Probability Value
Almost certain	Several times a week or day	5
Likely	More than once per month	4
Moderate	Up to several times a year	3
Unlikely	2–5 times every 5 years	2
Rare	Unlikely to occur	1

Then for each pair of threat and vulnerability we identify the possibility of detection and assign a rating in a scale of 1 to 5. However, here the lower the possibility of detection, the higher the rating and the higher the possibility of detection the lower the rating, as shown in Table 5-6.

Table 5-6. *Possible Detection Ratings*

Possibility of detection	Description	Probability Value
Extremely Low	Probability of detection is 0 to 20 %	5
Low	Probability of detection is 21 to 40 %	4
Medium	Probability of detection is 41 to 60 %	3
High	Probability of detection is 61 to 80 %	2
Extremely High	Probability of detection is 81 to 100 %	1

Once all three (total asset value, probability of occurrence and the rating for the possibility of detection) are determined for each of the threat and vulnerability pairs, then the risk exposure is quantified using the following formula:

```
Risk Exposure = Total Asset Impact Value x Probability of Occurrence x Possibility of Detection
```

The organization should have decided the risk exposure it considers as acceptable as a part of the risk assessment methodology adopted by it. It should not be too high that it leads to acceptance of every risk and it should not be too low that it leads to compulsory mitigation, avoidance, or transfer of every risk. Organizations are free to set their own acceptable risk xposure threshold depending upon their risk appetite.

Risk Responses

For each pair of threat and vulnerability, the calculated risk exposure is compared with the risk exposure considered acceptable to the organization (i.e., acceptable risk exposure). Where the risk exposure is less than the acceptable risk exposure, the risks are normally accepted by the organization and no further action is taken.

Acceptable risk exposure is decided by the organization as per its risk assessment methodology. Normally, this is the value of risk exposure below which the organization perceives the risks need not be focused on as the risks are very low and not worth pursuing.

There may be some other risks that the organizational management may want to consciously accept, such as the organization may allow mobile phones with cameras to be brought into the organization even though there is a risk that the cameras may be misused. The risk exposure in this case may be more than the acceptable risk exposure value. But, the organization may want to accept the risk because of its belief in the employees, considering other positive uses of mobile phones, not to demotivate the employees. Such practices of accepting the risk or not accepting the risk based on a specific context differ widely from organization to organization. As we have seen, some organizations may be very conservative in accepting the risks whereas other organizations may be relatively liberal in this regard when it particularly relates to inconveniencing the employees.

If the risk exposure is more than the acceptable risk exposure value then either the risk has to be avoided by mistake proofing (i.e., by implementing such measures that eliminate the possibility of such a risk occurring at all, such as if there is an unused entry or exit – mistake proofing is done by locking and sealing it permanently), the risk has to be transferred to others, or the risk has to be mitigated. Some of the possibilities of the transference of risk is to take up insurance for the risk of loss from fire or transference of risk of ineffectiveness or inefficiency through outsourcing of the work to the experts in that area. However, transference of risk is not possible in most of the cases.

Where the risks are not possible to be either avoided or to be transferred then they need to be mitigated. Mitigation is carried out by determining additional controls to be implemented. These controls may be awareness training, or may be implementation of a tool to monitor and provide alerts so that timely actions can be taken, or may be implementation of methods and techniques like encryption, or may be implementation of a security certificate for the URL, or may be introduction of additional validations and / or exception flows in the application software, or implementation of better processes. The additional controls implemented should be such that they have either the capability to reduce the probability of occurrence or reduce the impact or increase the probability of detection or a

combination of these. These additional controls or actions implemented should have to be assigned in such a way that there is high probability that the risk exposure is reduced below the acceptable value of risk subsequent to the implementation of the additional controls. All the additional controls to be implemented including the risk avoidance and risk transfer actions have to be assigned to relevant owners for effective actions.

Perceived risk exposure post implementation of additional controls should be collated against the existing risk to understand whether the additional controls are likely to bring the risk below the acceptable risk exposure value. Where it is perceived that the additional controls are unlikely to reduce the risk exposure below the acceptable value, the risks are to be brought to the attention of senior management of the organization and approval has to be obtained for bearing the residual risk.

Execution of the Risk Treatment Plans

The risk treatment plans (actions on account of earlier steps) are assigned through an Excel sheet or organizational action tracking tool to the respective owners and are tracked through the same on a regular basis. It is essential that the requisite focus and attention is provided by the management to ensure that these actions are invariably taken. Otherwise, the entire risk management exercise will be futile. Risk owners not only execute the necessary actions, but also ensure that the necessary processes to implement them effectively are defined and everybody (as relevant and required) is trained on those processes. Awareness of the risks and the actions required to be taken by all (as relevant and required) are also made known to everybody. The assigned action owners, upon implementation of the actions, check for the revised probability of occurrence, revised impact rating, and revised rate of detection. Where the risk exposure upon effective implementation of controls has not led to lowering the risk exposure below the acceptable risk value, then additional controls have to be implemented. Management has to be kept informed of the necessity and implementation of such actions so that requisite resources are deployed and the support is accorded for their effective implementation.

The Importance of Conducting a Periodic Risk Assessment

The organizational risk scenario changes when the business changes, the infrastructure changes, the technology deployed changes, and the competence of the personnel changes. These changes cannot be ignored, as these have the potential to impact the effectiveness of the controls already implemented and change the earlier risk profile of the organization. Whenever such significant changes are carried out by the organization or on a periodical basis (ideally on a six month to maximum of annual basis), re-risk assessment has to be carried out across the organization, and additional controls as required have to be determined and implemented. Proactive approach in this regard ensures that the effectiveness of the controls is maintained.

Figure 5-2 shows detail from a template that may be used for a risk assessment.

Figure 5-2. *Risk Assessment Template (detail)*

Incident Response

Before we discuss incident response, we need to be able to differentiate between three aspects: information security weakness, information security event, and information security incident.

To cite an example, suppose an employee tailgates another employee without swiping in his access card. This is a security event but cannot be considered as a security incident as the employee would have otherwise also come inside by obtaining a temporary access card if he had forgotten his access card. Suppose the tailgating is done by an ex-employee or a stranger. Then it is a security incident as it has the potential of leading to loss or disruption etc. Information security weakness in this case may be that once the employee has swiped his access card and gets into the organization the door takes a lot of time to close and lock down. Information security weakness may be that a utility you are using in the organization has a security loophole. Information security weaknesses if left unattended may lead to information security incidents. All the information security events may not be information security incidents but need to be evaluated to check whether they point towards a possibility of an information security incident. For example, a log shows that somebody was trying to access one of our servers from outside the organization. On checking, you may find that it was one of the employees who had authorization to have access to that information. Hence, it was an information security event which you cannot ignore, but upon evaluation you found that it is not an information security incident.

Potential security incidents need to be proactively protected against but some of the security incidents cannot be protected against like the unknown vulnerabilities in an application or operating system or a new virus or worm attack. However, where it is not possible to proactively protect against these we need to have alerting or detective mechanisms which alert us to the possibility of a security incident. For example a newly downloaded program is behaving suspiciously as found by your anti-virus or anti-malware tool. You need to check for what kind of suspicious activities are carried out by it, where it was downloaded from, and whether it is performing as intended, before you decide to act on it. Firewalls, IDS/IPS, anti-virus, and anti-malware software are some of the tools / utilities which provide you detective controls.

Once a security incident is identified, it cannot be left alone without attending to it. If the security incident was the tailgating by an ex-employee / a stranger or an application functionality behaving erratically, then the security incident has to be investigated to find out the root cause(s) for the same, so that corrective actions can be determined and taken to either fix the root cause(s) or mistake proof the issue itself.

If the incident is a serious one like a worm attack or a virus attack with serious implications then the actions or response has to be quick to contain the issue from spreading and containing the consequential damage.

In view of such a serious situation, having an effective incident response is necessary for all organizations. In order to achieve this objective, all organizations need to follow a well ordered Incident Response Life Cycle and have a comprehensively detailed Incident Response Plan. Incident Response Life Cycle defines various phases through which an incident has to be managed for incident responses to be effective not only in containing and spreading the effects, but also avoid recurrence of same or similar incidents. Incident Response Plan is the output of the Incident Response Preparation Phase and provides a well thought-out and well-articulated Incident Response Plan which enables the organizations to deal with incidents effectively and efficiently.

Figure 5-3 illustrates the Incident Response Life Cycle.

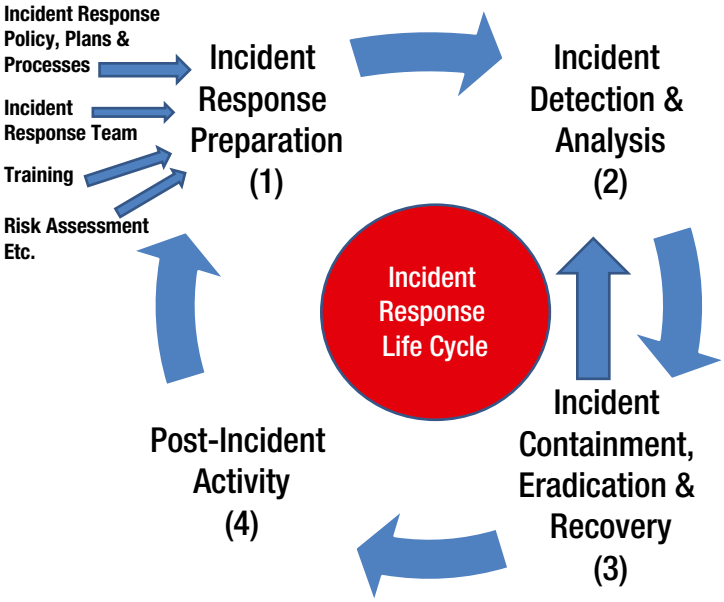

Figure 5-3. *Incident Response Life Cycle*[2]

Incident Response Policy, Plan, and Processes

Incident Response Policy should be put in place by management of the organization demonstrating its commitment to the Incident Response. This policy directs and provides guidance to the entire organization and provides the base for the Incident Response Plan and related processes.

Incident Response Policy

Incident Response Policy provides management direction towards Incident Response and also emphasizes the management's commitment to the same and highlights the "musts" as far as Incident Response is concerned. Incident Response Policy covers the following areas.

Purpose and Scope of the Policy

This should clearly define the purpose of incident response, namely, what the organization wants to achieve through incident response. This should also describe the scope of incident response in the organization. The scope can be the entire organization or a particular unit or a specific group of units and the type of incidents and circumstances.[2]
It highlights management's commitment and addresses what the management feels as mandatory to be followed with regard to incident response.

Definition of Information Security Incidents and Related Terms[2]

From organization to organization, the definition of information security incidents can differ. It is necessary that the organization clearly defines what it means by an incident and related terms like incident response, incident recovery, and incident response team.

Organizational Structure, Roles, Responsibilities, and Authorities

Any policy cannot be implemented effectively and efficiently unless there is a proper structure to support it in the organization. The structure should be composed of clear roles with clear responsibilities. For an incident response, many times somebody needs to act expeditiously without any bureaucratic approval cycle in order to carry out immediate containment or control activities. Therefore it is necessary that some of the roles have to be provided with authorities which may be beyond their normal authorities. An organization's structure, roles, responsibilities, and designated authorities have to be clearly defined and described so that there is no ambiguity, and that no confusing actions are taken.

All the people in the organization have to be clearly informed of the organization structure, roles, and responsibilities as the incident response has to be quick and requires coordination between various functions and personnel of the organization and cannot happen without this clarity across the organization. Otherwise, egos and organizational bureaucratic setups can create hurdles during an incident response which can delay the response significantly leading to a higher level of disruption or damage or theft. The roles, responsibilities, and authorities should provide the authority to the incident response team even to confiscate the equipment or disconnect the equipment and to monitor and investigate suspicious activities.[2] This also should make it clear what and which types of communications to the outside world or to the related agencies are permitted and who is permitted to carry out the same.

Incident Response Teams constitute personnel with complementary skills, experience, and capabilities. Head of the Incident Response Team is normally vested with significant authority to make decisions at times of need to effectively contain and recover from incidents.

Ratings of Incidents

All incidents do not require the same level of attention. Some of the incidents may be localized incidents and may have a local impact. Some may be organization-wide incidents with organization-wide impact. Some incidents may impact critical business areas and others may impact non-critical business areas. Some incidents may be easy to be responded to while some others may be very complex which can be responded to only by experts. Some incidents may have high impacts and some incidents may have low impacts on the organization. In order that the organizational personnel and the incident response team do not get confused, clear guidelines have to be provided as to the severity of various types of incidents. Speed of action required to be taken and the priority depends upon the severity rating of the incident.

Measurements

Any critical activity in the organization has to be measured to understand either its effectiveness or efficiency or both of these. The measurements provide us with the clear view of where we stand with respect to performance and bring out the opportunities for improvement. But, measurements to be made should be appropriate and should be defined in clear terms so that the measurements actually provide us the information as per the intended objectives of these measurements.

Incident Response Plan

The Incident Response Plan should clearly define what is considered as an incident in the organization. Second it should clearly identify the potential types of incidents the organization is exposed to based on the infrastructure of the organization, IT architecture of the organization, types of operating systems, and tools and utilities used by the organization. Third, it has to clearly describe what needs to be done if a new and unanticipated incident is faced by the organization. This may include who needs to be notified, and who will make a final call as to what needs to be done. The Incident Response Plan also has to specify external agencies or forums if any need to be informed or consulted with.

The Incident Response Plan covers the following areas.

Purpose and Scope

Purpose of the Incident Response Plan and the scope as to which type of incidents, pertaining to which location and which functions is made clear in this section.

Strategies, Goals, and Approach to Incident Response

Incident response strategies, goals, and approaches including the incident monitoring strategies, incident response strategies, strategies related to organization to effectively handle incidents including the team composition, internal and external coordination, and total or partial outsourcing of the incident response need to be clearly planned for and appropriate responsibilities are to be assigned to named personnel with appropriate backups so that there is a guarantee that in case of any incidents, they are handled effectively.

Internal and External Communication Plan

The communication for identifying the incidents, declaring the incidents, and responding to the incidents needs to be clear and should come from the persons authorized to carry out such communications. The communications should be within the defined boundaries and the communications should be appropriately worded. The clarity as to how internal communications need to be handled and how the external communications need to be restricted are to be clearly planned for.

Plan for the Incident Response Capability[2]

An organization requires adequate, suitable incident response capability in order to be effective and efficient in incident response. Any organization has to assess its current incident response capability in terms of availability of techniques, tools, and utilities and the resource competence including the skills to handle incidents. If it does not have the internal capability either the option to outsource or to acquire the capability through new recruitments has to be looked into. Plans to have appropriate, adequate, and suitable incident response capability have to be clearly delineated with action responsibility and target dates clearly assigned.

Measurement of Incident Response Capability and its Effectiveness

It is necessary to measure the incident response capability of the organization including that of the outsourced portion of the incident response capability. Periodic assessment of the same will close up the gaps between the expectations and the current realities. Organizations are not static. People with expertise and assigned key responsibilities may leave the organization. The same holds true for outsourced organizations.

At the time of outsourcing, the particular organization may have excellent capabilities but over a period of time it is possible that it would have lost the capability or would have had its capability reduced because of the attrition of key people. Further, the new technologies being implemented or changes to the technologies being implemented can make the requisite incident response capability differ from what was originally planned. Further, we also need to measure the effectiveness of the implemented capability. These may be possible to be measured by the responses that have been provided to the incidents which have occurred. Similarly, it may be possible to test some of the incident response through mock scenarios and testing of the possible incidents.

It is important to consider the various types of incidents possible and how they have to be handled so that there is no ambiguity. At least processes have to be clearly defined in respect to high impact incidents. These may be based on the common attack vectors.

Integration with the Other Plans of the Organization

An organization may have other plans like Risk Management, Disaster Recovery, and Business Continuity Plans. It is necessary that all these plans are integrated in such a way that each plan complements the other plans and does not contradict the other plans.

Incident Response Processes

Incident response processes are the important elements for the success of the incident responses. Various possible incidents from virus infection to malware infection to server crashes to denial of service attacks to bomb threats to many such possible incidents have to be thoroughly planned. Where the possibility of these incidents is high, the incident responses have to be discussed and planned for by having appropriate incident response processes.

These processes have to be detailed enough with various possible scenarios and appropriate responses. These processes have to detail how these incidents are identified and analyzed. These need to be supported additionally by templates, forms, and checklists as relevant so that it is easy to implement the expectations of these incident response processes effectively.

Incident Response Teams

Incident Response Team(s) is/are an important component and highly influence the success or failure of the effectiveness and efficiency of the incident response. This team requires the knowledge, experience, and skills to ensure that the incident detection, incident containment, and incident eradication are carried out effectively and efficiently.

Incident Response Team(s) can be dedicated teams or may be "on call" teams depending upon the criticality of the business, exposure of the organization to the incidents, competence of the IT resources, and resilience of the information security infrastructure.

Incident Response Team structuring based on distribution of the Responsibilities

Incident Response Teams are normally structured based on best fit distribution of the responsibilities among various centers.

Centralized Incident Response Teams[2]

Centralized Incident Response Teams are usually suitable for smaller organizations with less geographical spread. In big organizations such a structure can lead to lack of effective coordination due to various reasons like cultural reasons, internal political reasons, and bureaucratic decision making.

Distributed Incident Response Teams[2]

Distributed Incident Response Teams are suitable for multi-business, multi-locational organizations with distributed IT infrastructure. Each of these centers or group of centers may have their own Incident Response Team. In today's world, where each center is connected to the other centers and where the same business is carried out in various geographies and where the IT infrastructure is distributed based on efficiency and competency, it is necessary to have a person or group coordinating the efforts of these various Incident Response Teams as the same incident may affect multiple locations or an incident at one center may impact the business carried out at other centers.

Hybrid Incident Response Teams

It is possible that the expertise to handle the incidents in not uniformly distributed across various locations of an organization. In such a case it is possible to constitute a Central Incident Response Team at the prime location of the organization or technological hub of the organization with Incident Response Teams at the other centers as required. Incident response for some of the smaller centers or the centers which may lack the requisite expertise may be directly taken care of by a Central Incident Response Team. In such a model, it is possible to authorize the individual Incident Response Teams at various centers to act independently in case of local incidents and keep such incidents reported to the Central Incident Response Team. But, in case of purely local incidents the Central Incident Response Team assumes the advisory role if any support is required by the local Incident Response Teams. All the incidents which have impact across the businesses or locations or of higher impact are handled by the Central Incident Response Team. Necessary actions are directly taken by the Central Incident Response Team or as per the directions of the Central Incident Response Team by the distributed Incident Response Teams.

Incident Response Team Structuring Based on who Constitutes the Teams

The teams have to be constituted with appropriate competent resources. This depends upon the business, technology infrastructure, tools, and utilities used. If the team is not composed of competent resources it is possible that incidents may not be recognized sufficiently early or incident response may be delayed or incident response may not be effective. All organizations may not have in-house competence for effective and efficient incident response. They may have to complement internal competence with external expertise to effectively deal with incident response. Again the Incident Response Team can be constituted with full-time members or part time "on call" members. This depends upon the business criticality as well as IT infrastructure robustness, probable incidents, and IT resilience. The pros and cons of each of these structures have to be evaluated in the context of the organization and then an appropriate decision has to be made based on the well-evaluated and well-considered trade-off [3].

Fully Employee Constituted Incident Response Teams

If the organization has adequate internal competence then the Incident Response Team can be constituted internally. But, if the Incident Response Team is required to be available 24x7 and required to be deployed as it is, it is better to constitute a separate Incident Response Team with the experts specifically recruited by the organization. However, if it is enough to constitute an "on call" Incident Response Team then it is more effective to constitute the team internally with the expertise already available in-house.

Fully Outsourced Incident Response Teams

Here, the organization arranges for the entire team to be constituted by outside experts. Usually this may be through a single outsourced entity. However, it may be a group of organizations to which the outsourcing is done with complementary expertise, even though such a scenario is seen less in practice. This type of team constitution is usually found in smaller organizations for which it is difficult to internally source the requisite expertise. It is possible that such teams may have a tough time providing for effective and efficient Incident Response sometimes because of bureaucratic responses or hindrances or because of lack of effective authority delegated to them.

Hybrid Teams: Partially Constituted by Employees and Partially Constituted by Outsourced Contractors

Here, the organization constitutes its Incident Response Team with chosen internal employees and chosen outsourced contractors. This model is likely to work the best because the internal expert resources are complemented through other rare / non-available skills from the outsourced contractors. As the internal employees constitute a good portion of the team bureaucratic hindrances or lack of authority impeding effectiveness and efficiency of the incident response may not be an issue in this case.

Ensuring Effectiveness of Incident Response

As discussed earlier, incident response is not always easy for the following reasons:

- The actual incident may be the one that was not anticipated
- Key members of the incident response team and their backups may not be available when the incident actually happens
- Incident response plan is beautifully drafted but the stakeholders are not trained effectively on the plan
- Incident response teams are not staffed suitably or adequately
- Incident response plan was not updated for a long time and has become non-useful because of the changes to the infrastructure and systems over a period of time
- Incident Response Processes are outdated and are not in sync with the currently deployed technology

For effective incident response execution the following steps have become essential:

Preparation[2]

Any battle is half won before it begins if the preparations are done well. Similarly, preparation is very important to ensure the effectiveness of the incident response. Following are the important aspects of the preparation:[2]

- Risk assessment and identification of the risk mitigation steps to overcome the non-acceptable risks including the threats likely to lead to incidents
- Training the resources on the possible incidents and providing them the awareness and knowledge to enable them to effectively prevent the incidents, such as virus prevention programs, strong password, or encryption training
- Effective formulation of the Incident Response Team constituting suitable and appropriate structure and members with the requisite capability
- Well thought out and preventive IT infrastructure and physical security infrastructure
- Effective Incident Response Policy, Incident Response Plan, and supporting Incident Response Processes
- Validation of the Incident Response Plans and Incident Response Processes to ensure that they work when required
- Training on the execution of the Incident Response Plans
- Regular update to the Incident Response Policy, Incident Response Plan, and Incident Response Processes in tune with the changes to or at the organization
- Configuring the setup including those of tools / utilities used by the organization appropriately

Important aspects to be considered during the preparation are:[2]

- Internal and external contact details including those of on-call members, Incident Response Team members, and external agencies.
- Incident Reporting Mechanisms including the e-mail ids, contact phone numbers, or tools / utilities through which incidents can be reported.

- Incident Response War Room: This is the place designated for the Incident Response Team to operate. Primarily the Incident Response Team Leader directs and guides the team from here and can be contacted here. This room is provided with multiple telephone lines and other accessories to ensure effective communication in and out of this War Room.
- Incident Tracking Tool/Utility: Incidents need to be tracked including the status of the incidents and various actions taken at various places to ensure that the actions are executed as proposed. This is the incident repository which needs to be kept updated and which provides the Incident Response Team Leader to provide accurate and correct information related to incident status to internal and external stakeholders, as relevant.
- Readily available or accessible Incident Response Plan and Processes
- Secure Storage Facility: This is provided to store and preserve the evidence obtained during incident investigation.
- Mobiles or Tablets: These enable effective communication during the incident among internal and external stakeholders.
- Incident Analysis Hardware and Software such as Forensic Workstations, Backup Devices, Laptops and/or desktops, Servers, Portable Printers, Forensic Software, Digital Cameras, Video / Audio Recorders, Blank Media and other tools / utilities as relevant which help out in effectively analyzing the incidents; analyzing, collecting, and preserving the evidence.[2]
- Incident Analysis Resources including List of Ports, Network Diagrams / Maps, Configuration Management Database, Operating System and Database and Application related documentation.[2]
- Incident Mitigation Software which enables restoration and recovery of Operating Systems, Applications enabling IRT to create clean OS and application images.

Incident Detection[2]

Incident detection[2] is the next important step. All the incidents are not possible to be anticipated. However, there are some common threads among certain groups of incidents and these are normally known as Common Attack Vectors. These Common Attack Vectors enable us to understand and use the possibility of providing more specific responses. Table 5-7 lists the Common Attack Vectors.[2]

Table 5-7. *Common Attack Vectors*[2]

Common Attack Vector	Description
External / Removable Media	An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures)
Web	An attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware

(*continued*)

Table 5-7. (*continued*)

Common Attack Vector	Description
Email	An attack executed via an email message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message
Impersonation	An attack involving replacement of something benign with something malicious—for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token
Other	An attack that does not fit into any of the other categories

Precursors and Indicators of Incidents[2]

It is most difficult to understand whether the incident is occurring or has already occurred and the type, extent, and / or magnitude of the incident. Precursors provide an indication that there is a possibility of an incident happening, such as if there is an email or telephonic threat to the organization, a terrorist attack, or there have been failed attempts made to break into a critical system.

Indicators provide the signals that the incident is either occurring at this point of time or has already occurred, such as file checksums do not match, some data is leaked and published on a public website, somebody has already defaced the website, an increased number of files are getting corrupted day by day, or higher than normal utilization of the traffic is observed. It is possible that some of these indicators may be false positives and would have happened because of an employee's unintended mistake which was not even observed by the employee concerned or because of a wrong restoration by oversight or a wrong update. We may not have either a precursor or an indicator in case of some of the incidents, such as a new exploit of a new vulnerability just uncovered by a hacker or a misconfiguration newly exploited by an internal knowledgeable employee.

However, these precursors and indicators, when available, provide us an opportunity to speed up our responses and many times provide us the opportunity to either stop an incident from happening or reduce the impact of the incident.

Sources of Precursors and Indicators

Some of the sources of the precursors and indicators are described in Table 5-8.[2]

Table 5-8. *Common Sources of Precursors and Indicators*[2]

Source	Description
Alerts	
IDPSs	IDPS products identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces false positives—alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.
SIEMs	Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on analysis of log data (see below).
Antivirus and antispam software	Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date. Antispam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts.
File integrity checking software	File integrity checking software can detect changes made to important files during incidents. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
Third-party monitoring services	Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other incident response teams.
Logs	
Operating system, service and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Organizations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate an incident.

(*continued*)

Table 5-8. (*continued*)

Source	Description
Network device logs	Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying network trends and in correlating events detected by other devices.
Network flows	A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts. There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX.
Publicly Available Information	
Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in detecting and analyzing new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities. Organizations such as US-CERT33 and CERT®/CC periodically provide threat update information through briefings, web postings, and mailing lists.
People	
People from within the organization	Users, system administrators, network administrators, security staff, and others from within the organization may report signs of incidents. It is important to validate all such reports. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.
People from other organizations	Reports of incidents that originate externally should be taken seriously. For example, the organization might be contacted by a party claiming a system at the organization is attacking its systems. External users may also report other indicators, such as a defaced web page or an unavailable service. Other incident response teams also may report incidents. It is important to have mechanisms in place for external parties to report indicators and for trained staff to monitor those mechanisms carefully; this may be as simple as setting up a phone number and e-mail address, configured to forward messages to the help desk.

Analysis of the Incidents:[2]

As discussed earlier, all the indicators at all times may not provide accurate information and may lead to false positives. Hence, the mere presence of an indicator is not sufficient to presume that an incident has occurred or is occurring. A suspected incident has to be analyzed based on the indicators and other related information and then the analysis has to be confirmed. At the same time, it is necessary to understand the cause of the incident (may be an intentional attack, may be a misconfigured system, may be an employee mistake, may be unintentional violation of a policy impacting the system, etc.) to effectively deal with the incident. Many a time, experts may have to be involved in the analysis of the incidents to understand the correct causes and to arrive at effective solutions. Sometimes it may be too late to do anything as the confidential information is already released to the public. Sometimes only partial containment is possible. However, corrective action should be identified to either remove the possibility of such an incident happening or the possibility of root cause(s) from happening.

Table 5-9 details actions that may help in simplifying incident analysis, or making incident analysis relatively easy.[2]

Table 5-9. *Actions that may help in analyzing incidents effectively.*[2]

Action	Description
Profiling of Networks and Systems	Profiling is measuring the characteristics of expected activity so that changes to it can be more easily identified. Changes possibly indicate an incident even though sometimes these may be false positives.
Understanding Normal Behaviors	Study of networks, systems, and applications to understand their normal behavior will provide us sufficient clues to understand and identify abnormal behavior.
Creating a Log Retention Policy	Log information is critical information. This will provide leads into possible threads from earlier activities like reconnaissance activities. Having the logs for sufficient lengths of time ensures that there is a traceability to the thread of related activities as some of the incidents may be uncovered after substantial time of its occurrence.
Performing Event Correlation	Events can be correlated from different sources of information e.g. firewall logs to server logs to the application logs.
Clock Synchronization	Clock synchronization across all the physical and logical systems ensures that the incidents and evidences can be correlated easily. This provides adequate strength to the evidence collected from the legal stand point.
Maintaining and Using a Knowledge Base	This knowledge base acts as a quick reference source for the incident handlers. It should be easily searchable database. This knowledge base needs to be maintained updated with changes to the same in tune with the changes to the organizational scenario.
Using Internet Search Engines for Research	In today's world, Internet acts as a very important source of quick reference and useful information. We should be careful to ensure that the information is authentic, useful and relevant in the context of the incident faced by us.
Using tools / utilities as relevant	Use utilities like packet sniffers as relevant to collect more data to provide adequate information on the incident so that the action to be taken can be understood clearly.
Filtering the data	Various tools and utilities like SIEM, IDPSs etc. collect huge amount of data. It is not possible to go through each of these data. Data need to be filtered suitably and appropriately to identify possible patterns and possible indicators.
Seeking assistance from others	Various governmental and non-governmental sources can provide us information as to the current incident scenarios which may be applicable to us also. Keeping in touch with other Incident Response Teams from other companies or governmental and non-governmental agencies / forums can provide us crucial inputs on recognizing the incidents as well as analyzing the incidents effectively. However, caution should be exercised as to when we need to share the information.

Incident Impact Analysis and Prioritization of the Actions[2]

An incident may have impact on the functional aspects or on the CIA (Confidentiality, Integrity, and Availability) aspect of information security or both on the functional aspects as well as the CIA aspect of information security. Higher the impact, higher shall be the prioritization related to the actions to contain or to recover from them. Recoverability effort is also one of the important aspects which drive the prioritization of the actions. It is possible to recover from some of the incidents very easily with low effort, such as an isolated breach of one of the non-critical servers. It may be very difficult to recover from some of the other incidents and it may take weeks to recover e.g. a major security glitch in the application which is deployed across multiple systems in the organization. Further, in some cases if the information is already compromised, such as confidential information stolen already made public, there is no way you can recover from the situation for that particular instance.

Incident Documentation and Incident Notification[2]

Complete details of the incidents have to be captured including the analysis details, causes identified, containment actions identified and taken, and corrective actions identified and taken. These details can be tracked through an online system wherein the incident handlers need to update the details as they proceed with the analysis and take appropriate actions. It is important to document online or through paper based records various information related to the incidents. These not only come in handy later come in the evidence to be produced before legal authorities but also as future knowledge base as to what were the indicators, what were the analysis details, what were the causes, what actions were identified, which actions worked and which did not, whether the containment was effective, and if so to what extent, what was the magnitude or impact of the incident, whether the recovery actions worked or not, etc. These are crucial knowledge from the future perspective. Hence, the documentation cannot be ignored. Similarly, updating the status of the incident regularly on the online system should not be forgotten as the Incident Response Team Leaders as well as other key stakeholders like CIO, Chief Information Security Officer, or Owner of the data or system compromised, may be reviewing the status online or Incident Response Team Leaders may use the status for internal and external communication. Any wrong communication gives the wrong impression about the organization.

All the relevant and identified stakeholders (i.e., internal as well as external), depending upon the incident and corresponding incident response plans and processes, have to be communicated with regularly on the incident and its status. Typical stakeholders for the incident reporting are Chief Information Security Officer, Chief Information Officer, Business / Data / System Owner, Other internal and external Incident Response Teams, Human Resources (in case of breaches by employees), Public Affairs department (incidents of public concern where the status need to be informed to the public or where the incident attracts adverse publicity), Legal Department (where there are legal implications of the incident or where the incident has to be dealt with legally), and other governmental agencies / departments as relevant.

Incident Containment, Eradication, and Recovery[2]

Incident containment is very important to limit the impact on the business. The containment actions may be disconnecting or isolating the infected system from the network so that it does not infect other systems. Subsequent to the containment or in conjunction with the containment eradication of the cause(s) of the incident has to be done by identifying appropriate corrective actions. If mistake proofing of the systems is possible, like reconfiguring the system and thus avoiding recurrence of the same incidents in the future, the mistake proofing has to be attempted. However, you may have to weigh the costs of actions against the benefits from the actions and the residual risks. Further, recovery has to be attempted to ensure that the systems are restored effectively to their original positions at the time of the incident, such as if the data integrity is impacted because of the incident, then the data has to be restored to the accurate data by either nullifying the impact of the incident or to the last known state of data with the integrity intact and further transactions have to be re-applied. If the availability of the data is impacted the system has to be restored so that the legitimate users can access the same, such as after a DDoS the access to the server / system is restored to the legitimate users. In case of impact on confidentiality, possible eradication may be removal of the published data from those sites which had published the same (possibly nothing much could be done if somebody had already copied the data from there). All of the three aspects are important to ensure the effectiveness of the incident response.

Containment Strategy[2]

Early containment is important to the success of effective Incident Response. Containment reduces the actual damage or inhibits the resources from being exhausted, such as delinking an infected machine limits the spread of infection to other machines or diverting the attacking traffic to a sandbox, which avoids a denial of service attack. Containment strategy shall be spelt out clearly so that the incident handlers do not get confused but have absolute clarity on what prioritizes the containment. Sometimes it may be dangerous to carry out the containment if the containment action may make malicious software to act differently or severely. Hence, containment action should be well thought out by the experts. Some of the criteria for containment strategy are:

- Possible damage if the containment action is not carried out
- Whether the damage is likely to be increased if the containment is not carried out
- Services assured to the customers
- Time and resources needed to implement the containment strategy
- Type of the containment solution (temporary, permanent, etc.)
- Likely effectiveness of the containment strategy
- Evidence preservation requirement (NIST's SP 800-61 Rev 2)

The containment strategy should be kicked in as early as possible if the damage is likely to escalate because of further compromises possible or is likely to spread significantly impacting other business areas. However, the downsides of a containment action, if any, have to be understood before applying the containment actions.

Evidence Gathering and Handling[2]

Evidence needs to be gathered from two perspectives: first to understand how the attack is happening and where the attack is happening, second is to capture and preserve the evidence if legal ramifications are there or a legal battle has to be waged against the incident subsequently. If the evidence has to be used for legal purposes, then the evidence has to be collected as per the legal requirements, according to the prior consultation and understanding from the legal experts. It is also necessary to document how and when the evidence was collected and how it is preserved, how it is protected. A chain of custody for the evidence with clearly documented handover should be preserved. It is also necessary to take a snapshot of evidence as early as possible before application of any containment action so that the evidence is of value during the legal proceedings.

Eradication and Recovery[2]

Eradication is carried out as soon as possible. Eradication is getting rid of the vulnerabilities exploited or infection, such as a virus that infected being deleted, the misconfiguration of the system which was exploited is corrected, the defect in the application which was exploited is fixed, the operating system weakness which was exploited is appropriately patched, and changing the compromised passwords. Understanding the cause(s) of the incident is very important to do effectively.

Recovery is restoring the system back to normalcy, that is, undoing the adverse effects of the incident by restoring back the crashed operating system, correcting the integrity of the database, restoring back the correct data if the integrity of the data was impacted, or setting right the parameters altered by the incident.

Also, it may be useful to ensure from the learning of the incident that better logging, auditing, and monitoring are built into the systems so that the future detection of such incidents is easy. Effective eradication and recovery is often not easy and takes time. Some of them require infrastructural changes which may need budgeting, proper impact study, evaluation of alternative tools, and a plan for implementation of the selected tool.

Once the eradication and recovery is completed, the compromised system(s) need to be monitored to ensure that the eradication and recovery are effective. This gives the assurance that the incident is either possible to be detected easily in the future if it repeats or such incidents are possible to be prevented.

Post Incident Analysis and Activities[2]

Every incident and the way it was handled, provides significant learning which cannot be lost. The learnings from each incident need to be captured and analyzed so that the learning can be applied to future incidents as applicable. Also, in case legal actions are to be pursued then the evidence has to be organized and submitted to the appropriate authorities so that the legal actions can be initiated and pursued effectively.

Analysis of Learnings

Analysis of the learnings has to be carried out at least in the case of major or critical incidents. Periodic analysis meetings can be carried out in respect of collation of the learnings from other incidents. Ideally all the stakeholders who were involved in the incident detection, incident handling, and incident response should be involved in the meeting. The entire incident has to be deliberated upon and the results have to be collated:

- What had happened and when?
- Whether all the contacts could be contacted or were there issues in reaching the contacts like wrong e-mail ids or wrong / old contact numbers or the resources had already left the organization?
- Whether the incident response processes were effective or had to be modified on the fly to handle the incident effectively?
- Whether the incident handling led to any side-effects or adverse impacts and if so, what were they and how could they have been avoided?
- Was there a better way to respond to the incident than the way it was handled?
- Was there a better way to organize the response team?
- What information was needed but was not available on time?
- What learning from this incident can be applied to avoid probable similar incidents?
- What precursors and / or indicators were useful in identifying the incident and which of these will be helpful for future?
- Was the internal communication and external communication effective? Were they useful? Are there possibilities to improve upon these?
- What utilities / tools are required to better identify, prevent, analyze, or handle such incidents?
- Data related to the incident like duration of the incident, efforts spent on various phases of incident handling, types of incidents and their categorization based on various aspects like attack vectors used, external / internal attacks, etc.

Many more such questions can be asked to understand what went right, what went wrong, what could be done differently or better going ahead, and how these learnings will be useful for the future.

Use of Incident Data[2]

After analyzing these learnings, the improvement activities based on these learnings have to be initiated which may lead to the update of the Incident Response Plan and Incident Response Processes. Also, awareness and trainings may have to be improved based on these learnings.

Further, where legal actions have to be initiated, the details of the evidence collected have to be submitted to the legal department so that they can arrange for the legal recourse.

Data collected during the incident analysis has to be retained for a sufficiently long period for the following reasons [3]:

- Some of these may be useful at a later period of time, as some of the impacts of the incidents which are not identified now, may be identified later
- Some traces of future incidents may be found or some activities which are precursor activities for future incidents may be possible to be correlated to at a later date

Disaster Recovery and Business Continuity

As we discussed in the Introduction to this Chapter, Disaster Recovery normally applies to the IT infrastructure and IT systems even though it can be applied by some organizations in the context of all disasters. Business Continuity as mentioned here below provides for continuity of business in the context of disasters as well as business recovery post disasters. Normally, Incident Response Mechanisms handle disasters of smaller gravity, particularly security incidents and Disaster Recovery and Business Continuity Plans address higher order disasters. An organization may have a single plan covering all incidents and disasters or may have different plans for different aspects. However, where the organizations have multiple plans, it should be ensured that the scope of each plan is clearly defined and there is no conflict between these plans, instead these plans complement each other. In the following sections, we discuss all the three plans: Disaster Recovery Plan, Business Continuity Plan and Business Recovery Plan. All of these plans form a single composite plan that is known as Business Continuity Plan.

How to Approach Business Continuity Plan

A clear approach to the formulation of the Business Continuity Plan ensures that it considers all the important aspects and according to the scope of the business continuity that the organization wants to achieve.

Figure 5-4 illustrates the three important components of an effective Business Continuity Plan:

- Disaster Recovery Plan
- Business Continuity Plan
- Business Recovery Plan

Figure 5-4. *Components of Business Continuity Plan*

Assign Clear Roles and Responsibilities

For any project to be successful, it is necessary to define and assign clear roles and responsibilities. This is true even in the case of the formulation of Business Continuity Plans. The important roles and responsibilities in the context of the formulation of the Business Continuity Plans are described in the following sections.

Sponsor

Any plan will not be successful if there is no top management commitment. It is necessary from the perspective of provision of resources, allocation of sufficient budget, and getting the requisite infrastructure that Business Continuity Planning effort has the concrete backing of the top management. Ideal sponsor for the Business Continuity Plan is the Chief Executive Officer or the President or the Vice President of the organization. In case of specific unit level plans it can be the head of that particular unit. Such a person should demonstrate not only his / her commitment through funding and provision of resources, but also by intervening and resolving any barriers to the effective formulation of Business Continuity Plans. The sponsor should discuss with the Project Manager and formulate the scope of the Business Continuity Plans so that the Business Continuity Planning Team puts its efforts in the right direction and without any ambiguity. Budget for the entire business continuity planning also should be decided and conveyed by the Sponsor to the Project Manager.

Project Manager

Formulation of the Business Continuity Plan should be treated like a project. Hence, there should be a designated project manager. In the context of the Business Continuity Plan this person is normally known as Business Continuity Planning Coordinator. Some organizations may call such a coordinator as Contingency Planning Coordinator. Business Continuity Plan formulation project should have a planned start date and a planned end date. The activities or tasks to be carried over this period of time should be clearly planned in the schedule with the responsibility clearly assigned to relevant and appropriate personnel. Dependencies between various steps or tasks or activities of the plan have to be identified. A tool like Microsoft Project Plan or any other scheduling software or tool should be of help to carry this out effectively. The Project Manager or the Business Continuity Planning Coordinator can be an external consultant or an internal employee with prior experience in such a plan formulation or may be an

internal management person supported by an identified external consultant. Communication Plan is an important component of planning for Business Continuity Plan formulation. It is the responsibility of the Project Manager or the Business Continuity Planning Coordinator to ensure an effective Communication Plan.

Business Continuity Planning Team

The Project Manager or Business Continuity Planning Coordinator in discussion with the sponsor or on his/her own should identify the team members who need to be part of the Business Continuity Planning Team. Ideally it should be a cross-functional team representing the members from the business, IT team, information security team, facility management and security team, human resources team, Sales and Marketing, Community Relations and Public Affairs, and Supply Chain / Purchasing, Finance. Experts or external consultants may also be included as part of the team.

Life Cycle of Business Continuity Planning

For Business Continuity Plans to be effective in addressing all the components of the plan including disaster recovery, business continuity and business recovery, organizations need to follow a well-defined Life Cycle of Business Continuity Planning. The success of the organization and its ability to withstand a disaster or serious business disruption depends upon the adequate thinking provided to each aspect of the life cycle, detailing of the same so that it is understood by everybody as relevant, tested for the assurance that it will work as expected in case of need and will enable the organization to bounce back effectively and efficiently on to the path of business continuity and business recovery. The Life Cycle of Business Continuity Planning is illustrated in Figure 5-5.

Figure 5-5. *Business Continuity Planning Life Cycle*

Scoping

Appropriate scoping is very important and the starting point of a good Business Continuity Planning exercise. Whether the scope is the entire organization, for specific location, for specific business, or for specific department should be clearly set by the Sponsor of the Business Continuity Plan in his / her discussion with the Business Continuity Planning Coordinator. The scope should be written down and signed off by the Sponsor to ensure that there is no disconnect between what was expected by the Sponsor and what was understood by the Business Continuity Planning Coordinator.

Plan for Formulation of Business Continuity Plan

A draft Project Schedule has to be prepared with a clear planned start date and planned end date. Various activities or tasks to be planned to formulate the Business Continuity Plan are identified. Assignments of the planned activities to various team members are also carried out. Dependencies between various tasks are also identified. Pre-requisites for important activities and success criteria for important activities are also identified. This draft schedule is discussed with the Business Continuity Team during the Business Continuity Plan Kick-Off Meeting and is finalized.

Communication Plan is an important component of planning for Business Continuity Plan formulation. This plan very clearly delineates how the status of the formulation of Business Continuity Plan is communicated to various stakeholders including the Sponsor and when and how the issues related to the plan are communicated. This plan also delineates channels of communication and various meetings that are part of overall communication strategy. This also includes the communication of any changes including changes to the scope, changes to the cost, and changes to the project plans. This draft communication plan is discussed with Sponsor to check that the plan is as per the expectations of the Sponsor. This plan is then discussed broadly during the Business Continuity Plan Kick-Off Meeting and agreed to.

Business Continuity Plan Kick-Off Meeting

This is an important meeting of the Business Continuity Planning Team wherein the scope of the Business Continuity Planning is discussed so that everybody on the team is clearly aware of the scope. The broad plan prepared by the Business Continuity Planning Coordinator will be discussed with the team and depending upon the team's views necessary additional tasks / activities are incorporated, timelines are revised, dependencies are added / modified, and the responsibilities for various tasks are reassigned where required.

This meeting also discusses the risks to the schedule, risks to the achievement of the objective of the plans, and risk of the resources planned to be employed (non-availability, over engagement in other critical activities etc.).

Any issues expressed by the team members are considered, discussed, and necessary actions to be taken are planned for / determined.

Business Impact Analysis (BIA)

Business Impact Analysis is at the heart of Business Continuity Planning. Data from various local agencies, regional agencies, national agencies, and international agencies, as relevant, are collected related to applicable disasters and taken into consideration during the Business Impact Analysis.

The first activity as a part of the Business Impact Analysis is to list out various Business Lines of the organization and to understand their relative contribution to the organization and their relative criticality in terms of revenue and profitability. This also has to take into account impact on the customers of those business and possibility of the customers moving to other organizations if they are not supported. Business Impact Analysis will allow an organization to determine as to how much time each of these business lines can be down without significantly impacting the customers, and also how much a reduced level of service can sustain the business for some time. Table 5-10 provides an example of how different lines of business determine the criticality of business continuity and recovery.

Table 5-10. *Criticality Analysis of Different Lines of Business*

Business Line	Business Share (% of total business of the organization)	Profitability %	Criticality of Business Continuity and Recovery
Business Line A	54%	12%	Critical
Business Line B	17%	18%	Critical
Business Line C	15%	5%	Non-Critical
Business Line D	14%	-2%	Non-Critical

Assurance made to the customers of various service levels, impact on the customers due to the business downtime / service downtime are taken into account and minimum time within which business needs to be continued even at the reduced levels of scale or reduced service levels have to be identified. This step is very crucial for the success of effective business continuity.

Then we look at the risks to the systems enabling and supporting each of these business lines including IT infrastructure, software, applications, tools, and utilities from various applicable threats or scenarios including from natural disasters, infrastructural breakdowns, riots and strikes, system downtime because of issues like virus infection, and server crashes. We identify the top risks based on their probability of occurrence and their likely impact on each of the business lines. We use the data available while arriving at these. The focus here is on availability as this is the risk we want to cover primarily as part of BIA. However here, we go beyond the normal risk assessment and assume that the disaster is likely to happen and think of what steps the organization needs to take to recover from disasters and continue the business if the disaster comes true in spite of controls put in place.

On the basis of the criticality of various Business Lines and the corresponding applicable risks or scenarios, relative ranking is used for prioritization of recovery and focus on business continuity. This step is very crucial for the success of effective business recovery. Additionally, it is good to understand, at this point in time, the implication of downtime or disruption on the confidentiality, integrity, and primarily availability (as BCP addresses primarily the issue of availability). The same guidelines from NIST's FIPS PUB 199 as used in the Risk Management Section may be referred to understand the impact. The rating may be 1 or Low; 2 or Moderate; 3 or High i.e. one in a numerical scale and the other at risk level.

From the above the following three important aspects of Business Continuity and Recovery are decided:

Maximum Tolerable Downtime (MTD): This is the downtime or outage or disruption considered as tolerable by the stakeholders particularly business users in the context of a specific business line. Beyond this period of downtime, it will be perceived that the downtime will have severe impact on the business. This provides the inputs for the recovery method and processes to be used.[4]

Recovery Time Objective (RTO): This is the maximum time by which the recoveries of the affected systems have to be accomplished. This provides the input for the technologies to be used for effective recovery. This has to be less than the MTD as the recoveries of the systems well before the MTD are necessary to ensure that the business can be carried out effectively after MTD. Further, testing of the integrity of the system and data restored shall also be checked and ensured before MTD. This provides for time to get a new server (rented or redeployed within the organization or leased etc.), install the operating system, install the application, configure the system appropriately, restore the backup from the backup media, check the system for effective restoration and roll it out for production, etc. Where the RTO is more than the MTD, then the Top Management has to be consulted as to the risks to the business and necessary steps as required have to be planned for as per the guidance of the Top Management.[4]

Recovery Point Objective (RPO): This is the point of time before the disaster or disruption or outage that the system can be brought back to. This applies to the data and usually depends upon the number of hours of data we can afford to lose. This decides the required backup frequency and type of backup. If the data is critical and can't be lost at all, then online real-time mirroring of the data may have to be looked into. However, whenever strategizing such things the cost vs. benefits have to be considered.[4]

The analysis that we've discussed is better known as the Business Impact Analysis (see Figure 5-6). Typically, the organization determines five business areas and five relevant disasters (as per the thumb rule), which need to be addressed for business continuity as well as recovery. This number may vary from organization to organization; however, looking to continue all the business lines, and always at the same level of performance, is possible to achieve only at high redundancy. It requires a high investment to support business continuity, and may not be a prudent business decision. As mentioned earlier, based on the relative criticality of the selected business lines, the recovery and continuity efforts are prioritized. Consequently, critical systems supporting those business lines and the priorities for their recovery also are identified.

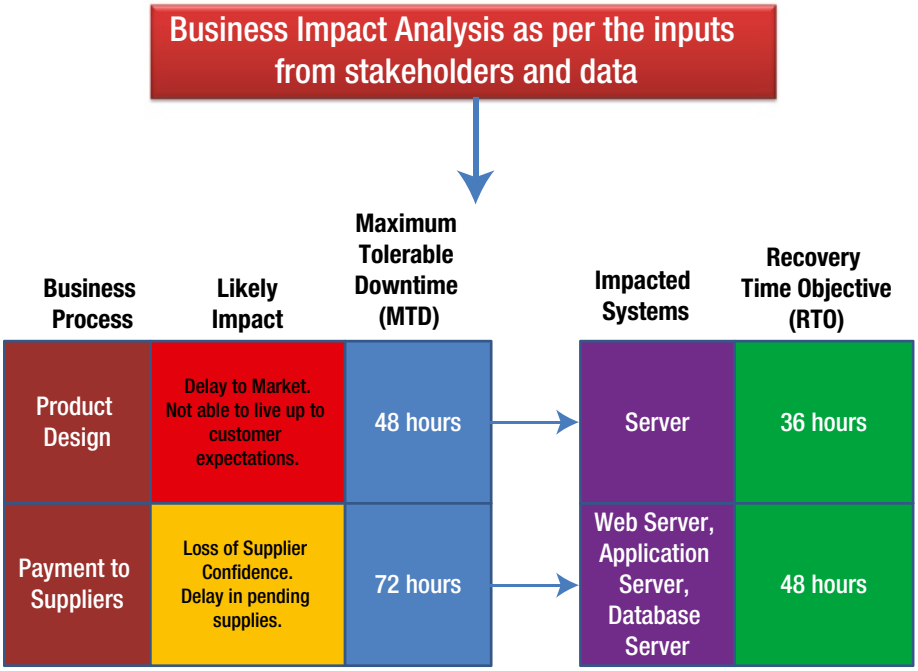

Figure 5-6. *Business Impact Analysis*[3]

For some customers or some businesses, it may cost significantly if the business doesn't continue at the time of disaster or as early as possible after the disaster. For example, e-commerce business with high competition and huge volumes of business may lead to huge losses or potential business losses even if the systems are out for part of the day. Hence, we need to identify the need for continuity of business while recovery efforts are underway.

Adequate and appropriate resource deployment is the next important step in the process of effective recovery. Facilities, staff, hardware, operating system and other software, application software, data, tools and utilities, and relevant records are the important resources required to ensure effective recovery. These should be identified well ahead of time in appropriate quantity with appropriate capability to ensure effective and efficient recovery.

Again, while most focus is on recovery, as discussed earlier, not all business lines may require continuity of business immediately after the disaster as this can be enabled in case of most disasters only at a high cost like hot sites setup and maintenance.

Whether the business can be continued at a lower scale from the same site or from another alternate site depends upon the type of disaster impacting the current site. Heavy floods or huge fires or earthquake, or damages on account of terrorist strikes through bombs etc. may lead to total or high devastation at the current site and hence it may not be possible to recover the services mostly within the MTD from the same site. Hence, in case such disasters are perceived strongly (i.e., with relatively high probability), then business continuity or business recovery from other alternative

sites may have to be planned for. If the immediate continuity of the business from another site is required, then alternative hot sites may have to be setup. If the business can wait for some time, then there is a possibility to recover and continue the business from other alternative sites by having alternative warm sites. If there is substantial time available as MTD, then it may be enough to have a cold alternative site or a reciprocal arrangement with some other organization. These alternative sites may be the ones owned already by the organization or may be the sites leased out for the specific purposes of business continuity or may be the sites of other organizations with which we have reciprocal arrangements.

In most of the cases, the disasters may have localized impact in which case business may be possible to be routed temporarily through some other sites where possibly only the personnel have to be shifted temporarily along with the requisite equipment like laptops etc. Some of the cases can be handled effectively by having reciprocal arrangements with other organizations in a neighboring town or city which can be easily reached within a reasonable time-frame.

Business Continuity Plan Preparation

Once the business lines to be supported along with the applicable disasters and the corresponding systems to be recovered and / or business operations to be continued from alternative sites are decided along with the priorities attached to them, the detailed Business Continuity Plan is drawn up.

The Business Continuity Plan lists out the Business Lines determined to be supported (as per BIA) as part of BCP as per their priorities. For each of the business lines the top few identified and applicable disasters impacting them as determined during the BIA are listed out. Based on each disaster scenario, the systems to be brought up and the resources required for the recovery process are listed as determined during the BIA.

The next step is to identify the Preventive Controls. Preventive Controls are such controls which make it possible to reduce the impact or the possibility of some of these disasters, such as fire through mechanisms like smoke / fire detectors, fire alarm systems, and fire suppression systems. Many of these would have been considered as a part of organizational information security risk management activities. If not, possible preventive controls are now identified and assigned to appropriate personnel for effective execution.

For each of these listed disasters, what should be done during the first 24 hours, first 48 hours, first 72 hours of disaster are identified. These may be arranging for alternative servers, alternative routing of the network traffic, operating out of alternative sites (including where applicable other locations of the organization itself), restoration of the system files and data on to the alternative servers set up etc. The MTD and RTO are taken into consideration while planning these. The objective is to ensure that the business and supporting systems are brought back before the MTD. These have to be supported by effective and well-planned recovery processes.

Effective recovery depends upon the contingency strategies planned for. Some of the contingency strategies are backup and recovery methods, offsite storage strategies, provisioning of alternative cold, warm, or hot sites. Reciprocal arrangements for alternative sites, provision for receipt of backup equipment from the hardware vendor, inventory of internally deployable alternative systems necessary equipment to be stocked internally etc. are also required to be planned as part of these strategies. Service Level Agreements or timelines have to be agreed with suppliers, where appropriate, to ensure timely and effective support. All these should be in tune with the determined recovery strategies / plans and should support the RTO and RPO. These should be appropriately captured as part of the BCP. Cost vs. benefit analysis should be carried out while deciding these and appropriate strategies have to be selected keeping in mind RTO and RPO.

Outage assessment procedures like assessing the cause of an outage, potential impacts of the outage, damages possible to the infrastructure and systems, time required to bring back the situation to normalcy, and so on have also to be planned as part of the BCP.

Various recovery procedures and their sequence of execution have to be planned for in detail as part of the BCP or as addendum to the BCP or as a separate companion plan. Procedures to check the effectiveness of the recovery activities during the reconstitution phase also have to be planned for as part of BCP.

Various roles and responsibilities to effectively execute the Business Continuity Plan are determined and documented as part of the BCP. While BCP Coordinator plays an important role in the entire planning and execution of the BCP, there are other roles and responsibilities which are important to ensure effective execution of the BCP. One of these is the Crisis Management Lead who is the senior person from the organization who is empowered to

declare the situation as a crisis upon evaluating the scenario and the possible damages or impacts. Other roles may be the Travel Coordinator for arranging for travel during the disaster, Purchase Coordinator who initiates necessary purchases as per the plan, Facility Coordinator who sets up the alternative site / facility, Server Recovery Team, Network Recovery Team, Database Recovery Team, Legal Affairs Team, Public Affairs Team, etc. while the BCP Coordinator takes overall lead and provides overall guidance for the effective execution of the BCP. Also, backups for each of the critical roles is also decided and assigned as part of the BCP.

Crisis Communication and other communication plans are also part of the Business Continuity Plan. These very clearly describe who is empowered to communicate with the internal and external world on the crisis and what kinds of communications are normally allowed in case of the relevant disasters. Even the forms and templates as necessary to support the same may be provided. The line of communication chart is also provided as needed, if the communication at various centers has to be percolated down / to others through various personnel of the organization. Activation criteria for important communications like crisis announcement and various notifications to be provided prior to the disaster, during the disaster, or after the disaster are also documented clearly as part of the BCP.

The primary and secondary contact details like landline numbers, mobile numbers, e-mail ids, and addresses of personnel assigned with various roles are captured as part of the BCP. The contact names and details of various critical suppliers like offsite backup custodial service providers, critical suppliers to whom critical work has been outsourced, etc. are also captured as part of the BCP.

Designation of the war rooms and the facilities to be available in the war rooms, the type of documentation to be carried out during the entire BCP life cycle; who is responsible for the documentation as scribe, and so on are planned for clearly as part of the BCP.

The plan is concluded with all the necessary contents as above and reviewed with the sponsor for completeness, consistency and correctness.

Business Continuity Plan Validation & Training

The Business Continuity Plan has to be tested and validated to get the requisite assurance that it works effectively when required. Testing and exercises are part of this validation. This is an important step of the Business Continuity Plan and cannot be missed out.

Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. Testing should be performed as far as possible in an environment akin to the current operating environment of the organization. Each of the recovery processes mentioned in the plan should be tested to get the assurance that they work when executed. Some of the things tested as part of BCP validation are:[3]

- Notification procedures;
- System recovery on an alternate platform from backup media;
- Internal and external connectivity;
- System performance using alternate equipment;
- Restoration of normal operations.[4]

This testing has to be carried out methodically using the test plans with clearly defined test scenarios (ideally worst case scenarios) and success criteria based on the defined test objectives. Test Plans should also test for the time-frames for each of the critical processes. This enables us to understand whether recovery is possible as per RTO or not.

Based on the outcome of the tests, necessary modifications or improvements may have to be made to the BCP.

Training on the BCP has to be provided to various roles mentioned in the BCP. The primary focus should be on the objective of the plan, communications to be carried out by and among various roles including reporting processes, coordination between various roles, do's and don'ts, team specific processes, responsibilities attached to individual roles, and security requirements. All the stakeholders have to be involved in the training mandatorily and clarify their doubts so that they are effective when it comes to the execution of the plan in case of eventuality.

Various exercises are conducted to ensure that the plan is appropriate and works when needed. Some of the popular exercises used are:

- Table Top Exercise[4]: This is normally done as a class room discussion based exercise. Here, no equipment is used. Various stakeholders meet and discuss their responsibilities in the case of an emergency and how will they respond in the context of a specific scenario provided by the facilitator.
- Functional Exercise[4]: Simulated environment is used and emergency processes are implemented by various teams. The teams carry out their emergency responsibilities in the simulated environment. It provides them hands on experience as well as tests the validity of the plans and processes. These may be exercising specific responsibilities of specific team members or exercising specific processes etc. These may be limited to specific aspects of the plans or may be a full scale exercise of the plan.

Table Top exercises may be enough for low impact systems. Limited functional exercises may be required for medium impact systems. Full functional exercises may be required in case of high-impact systems.

Up-to-date Maintenance of the BCP

With significant changes to businesses or infrastructure or systems, the BCP need to be reviewed and the need for its continued currency or the need for update to the same has to be ascertained. In case, the changes have impact on the BCP, it needs to be updated. Where the changes to the BCP are significant, then re-training of the resources and re-validation of the BCP are important. Even in case the BCP is static in terms of its technical contents, the BCP may require periodical updates and trainings on account of changes to the personnel and their responsibilities, and contact details. Like the original BCP, modified BCP also has to be reviewed and approved by the Sponsor of BCP.

Chapter Summary

- We discussed security breaches on confidentiality, integrity, and availability aspects of information security. We also made it clear that the risk management, incident response, disaster recovery, and business continuity planning are critical to ensure that the impacts on or compromises to confidentiality, integrity and availability are reduced significantly. We also stressed upon numerous theories around these concepts and found that they are diverse and many a time confusing. We also defined some of the key terminologies used in the chapter in our simple and practical ways to avoid confusion to the readers.
- We explored Risk Management and looked at each of the components of the risk management life cycle including risk identification, risk analysis, risk response, execution of risk treatment plans, and periodical risk assessments. Each of these were explained and elaborated in detail. Detailed guidelines are provided so that the users can effectively carry out the risk assessment. A useful template for risk assessment is also provided as reference.

- We also explored upon the Incident Response Policy, Plan, Processes, and the Incident Response Life Cycle. We looked at the importance of the preparation activities. We elaborated in detail upon incident detection including incident analysis, incident containment including containment strategies, incident eradication, and incident recovery. We also explained how the post incident analysis like learning, use of data collected are important, and useful steps leading to the improvement to the incident response mechanisms.
- We examined the Business Continuity Plan (including the Disaster Recovery, Business Continuity, and Business Recovery). We elaborated upon the important roles and responsibilities related to the formulation of the BCP. We also elaborated upon the planning required to arrive at the BCP. We also examined, as part of the BCP Life Cycle, the importance of Business Impact Analysis, and how it becomes the base for the formulation of the BCP. We also looked at the broad contents of the BCP. We also highlighted the need for validation of the BCP through Testing and Exercises. We also explored how training helps in the effective implementation of BCP. Then we highlighted the need for keeping the BCP updated with the changes.