Vulnerability Assessments and Penetration Testing Overview

A security control cannot truly be trusted until it has been tested. A control is intended to mitigate a risk, but not all controls are effective, and a control may lose its effect over time. Regular (scheduled and unscheduled) reviews and assessments of an organization's security are essential to provide insight into the management of risk and effectiveness of controls. Management cannot provide good governance if they do not receive accurate and complete information from security assessment and audit.

The testing of controls may be conducted in several manners—aggressively trying to breach the control, or merely monitoring and passively testing the control. Security assessments may be done by audit, the security department, IT administrators, third party auditors, external penetration testers, and by management as part of a continuous monitoring process.

Testing of controls is often conducted using a variety of techniques. A manual test may be conducted using a human expert to probe for problems, or automated tools can be used that have the ability to process vast amounts of data and examine complex systems. A good test strategy is to conduct several types of tests and ensure that the personnel using the automated tools are well trained in how to configure and operate the tool and especially, how to analyze the results of the test. The results of the test also need to be communicated to management in a clear, understandable manner.

Security Assessments

The university professor told students that the purpose of testing a software application was to see if the application would fail, not to see if it worked. As we have all seen lately, many people can write programs that work, but many applications are not built to be resilient and robust enough to survive user error or an intentional attack. Users will input wrong data in the wrong field into a program. Attackers will try innovative ways to cause a program to fail in order to seek a way to compromise the systems and data that the application can access. Therefore, programs have to be written to expect an attack and resilient enough to manage errors and attacks without creating a security compromise. This must be remembered when conducting a vulnerability assessment: the purpose of the assessment is to find any vulnerabilities. It is only when an organization is aware of a vulnerability that they can take steps to mitigate the associated risk.

Vulnerability assessments and penetration tests are separate activities, but they work well together. A vulnerability assessment is often broader in scope and may cover all the attack surfaces of a system; whereas, a penetration test is often narrow in scope and focused on a specific area of risk. A vulnerability assessment may generate a lot of “noise” or false positives that can be examined in more detail by a penetration test, but a penetration test on its own may be so focused that it misses problems outside of the direct scope of the penetration test.

Either internal or external teams may conduct vulnerability assessments and penetration tests. In fact, it is recommended to use internal teams that know the systems well and external teams that attack a system using “fresh eyes.”

The security practitioner is often a part of a vulnerability assessment or penetration testing team. These teams require skilled staff that can assess a system from a technical approach and also from a non-technical approach. Testing a system requires the assurance that everything is secure, not just the hardware or application. For example, a test may examine a firewall and run various sets of test data against the firewall to ensure it blocks unacceptable traffic and allows acceptable traffic. However, the firewall also needs to be tested from a non-technical perspective. Review of managerial non-technical controls would ensure that administrators are adequately trained, there is a change control process to manage configuration changes to the firewall, and there is an analysis and reporting process to report on the operation of the firewall. That the firewall is installed with adequate power and physical security is part of a non-technical physical assessment. Management can only be confident in the effectiveness of the security program if the assessment considers all three (managerial, technical, and physical) elements of the control.

In other cases, a security practitioner may play a supporting role related to an assessment. The security practitioner could be responsible for allowing access, providing reports, and answering questions for the assessment team.

Once the assessment is complete, the security practitioner may be assigned to address any of the issues discovered during the assessment, such as applying missing patches or reconfiguring a device.

Testing Strategy

A test strategy ensures that all of the areas that need to be tested are adequately assessed. Test strategies may include using checklists or standards such as PCI-DSS that lists all of the areas to be examined. A test strategy looks at testing from the perspective of a normal user error and from the angle of the misuse case actor that intentionally is trying to compromise the system. Having a test strategy can also help ensure that tests are conducted in a consistent manner so that the results of one test can be compared against the results of previous tests.

The test strategy may also include the preparation of test data that can be used repeatedly. Test data should test all expected inputs—all allowable values—and also improper inputs to ensure that the program processes errors correctly and does not accept invalid input.

In order to facilitate the tests, the developer or vendor may put back doors (trapdoors) into their programs. These allow the dynamic testing of the software code and grant visibility into the actual data processing function. The problem is that sometimes an attacker discovers these back doors and uses them to exploit the application or system.

Vulnerability Assessments

A vulnerability assessment is used to detect potential vulnerabilities in a system, process, or organization. The assessment should include both technical and non-technical tests, using a combination of automated tools and scanners, manual processes, interviews, and data analysis. Surprisingly, many people have thought that a vulnerability assessment is strictly technical or exclusively internal. In fact, such tests would be inadequate to provide clear insight into the security posture of the organization.

A good analogy for a vulnerability assessment is the task of protecting a walled city. The captain of the guard must ensure that all elements of the defense are working correctly—the walls, gates, and drawbridge. The captain must also ensure that the guards are awake, trained, know how to detect an incident, and how to notify others in case of an attack. The protection of a walled city requires 360-degree assessment since a small breach at any point along the wall could lead to a serious compromise of the entire city.

This is similar to the approach used in a vulnerability assessment. The security practitioner should examine all aspects of network and system security to ensure that there are no breaches anywhere in the infrastructure. This can be done by performing network scans that will discover new equipment on the network and compliance scans that will ensure all devices are configured correctly and compliant with security baselines.

A vulnerability assessment is a fairly passive test in that it does not attempt to exploit any vulnerability, and it causes little impact on performance or system availability. However, like any test, it should only be conducted with management approval, and care must be taken not to interrupt system processes.

There are many tools that can be used to perform a vulnerability assessment, and lists are available that list known vulnerabilities. This allows the tester to test for those specific known vulnerabilities. Several sources are also available that list known vulnerabilities that should be reviewed.

Discussion: Conducting a Vulnerability Assessment

What tools and sources do you use that you recommend and find useful when conducting a vulnerability assessment?

Review: Conducting a Vulnerability Assessment

A key part of the vulnerability assessment is the gathering of data needed to perform the assessment. Data may be gathered using tools but also by interviewing users and administrators and reviewing error and outage logs, audits, or audit standards.

The results of the vulnerability assessment are documented in a report submitted to management for action. The report should indicate the severity of the vulnerabilities and recommended courses of action. Risks also may be added to the risk register for tracking purposes.

Penetration Testing

The disadvantage of a vulnerability assessment is that it often contains false positives—vulnerabilities that are not in fact true vulnerabilities. The analyst attempts to discover which vulnerabilities are real and which are not serious, but it can be difficult to know the severity of a vulnerability if it has not been tested. So, a penetration test attempts to break in to prove whether a vulnerability is a real problem or just noise.

A penetration test attempts to exploit an identified vulnerability to prove whether the tester is able to penetration the defense of the system and whether the systems controls identified and blocked the attack.

A penetration test tends to be much more aggressive than a vulnerability assessment. The tester will try to exploit a system. This does cause additional risk to the organization. All tests should be conducted with appropriate levels of management approval.

There are many tools used in conducting a penetration test and many of these can be dangerous. Such tools should be used only with permission from management, and care must be taken to avoid causing a system outage.

Zero Knowledge Test

A zero-knowledge test is done by an outsider (external tester). It assumes the position of a hacker from another country that has decided to attack an organization and only has access to materials that are open source or publicly available. This type of test most accurately simulates an attack by an external hacker, but also it is the most expensive in the time taken to perform the test. Many penetration-testing organizations are reluctant to do this type of test since it consumes resources and requires a higher level of skill than just a partial knowledge test being performed by a junior level tester running some readily available tools.

The secret to this test is to discover where information about the client organization may be leaking out that could be of an advantage to a hacker.

Partial Knowledge Test

This is the most common type of test. For this test, the client organization provides a penetration-testing firm with information that can be used in the test such as IP addresses, network layouts, and SSIDs of wireless routers. The penetration-testing company then has enough information to create a targeted test plan and focus on known vulnerabilities. This can determine whether the client organization is subject to these known types of attacks, but it may not find other problems outside the scope of the test.

Full Knowledge Test

This test is performed by an internal team completely familiar with the networks, applications, configurations, and culture of the organization. These tests are valuable to find any problems before a hacker does and to see if any security vulnerabilities or configuration changes have emerged that could subject the organization to an attack.

Blind Test

A blind test is conducted by a penetration-testing team without the knowledge of the IT department. This type of test determines whether the IT department can detect an attack and measures how well the organization responds to it.

Double Blind Test

A double-blind test is conducted by a penetration-testing team without the knowledge of either the IT or security department. This tests the incident management program and discovers whether the controls can detect a problem and whether the staff responds appropriately.

Summary

All of the tests performed on a system, an application, or a network should be complete and rigorous to ensure that any vulnerabilities in technology, processes, management, or physical security can be detected and mitigated.

Audit Findings Overview

Audit provides management with assurance on the effectiveness of the security controls and the risk management process. This gives management a sense of whether the security is adequate (commensurate with risk). Security will never be perfect, and it will require a continuous effort to measure and report on the status of the security program and the advancements being made to address outstanding issues.

Audits are to be conducted by independent and objective personnel with the required level of skill to conduct the audit in a professional and thorough manner. Audit risk is the risk that an audit missed a critical element of the audit and failed to detect a problem. This is serious since audit stands as the last resort for management, and a failure to provide the professional results would lead management to a false sense of security and possible complacency.

Either an internal or external team may conduct audits, but both are required to follow audit standards that address the conduct of the audit and the responsibility to report on any materiel findings.

The advantage of audit is that an auditor provides "fresh eyes" to look at a business process. This can sometimes uncover problems overlooked by staff that is busy in the area on a daily basis. The security practitioner will often have to assist the auditors by providing evidence or work papers that the auditor will use to analyze and assess the area under review. The security practitioner should be diligent to ensure that any information requested by the auditor has been provided in a complete and timely manner. When responding to audit requests, the security practitioner should be careful to follow normal procedures so that the audit is able to validate that the procedures are being followed.

Communicate Findings

Audit reports follow a standard format that gives management a consistent view of the audit. The report includes describing the scope and objective (purpose) of the audit, the findings of the audit, and the auditor's recommendations. Management may respond to the recommendations and pledge to address them in a set time period. The security practitioner may play a role is resolving or addressing any audit report findings.

The audit report is submitted in draft mode to management. This allows the direct managers involved to address any errors or incorrect assumptions in the audit and to provide a plan (schedule) to address the recommendations. In some cases, management may not agree with the auditor's recommendations and that will also be noted in the audit report.

Even if an issue is addressed before the final audit report is submitted, it is still important to record the issue in the audit. This allows the auditor to follow up and ensure that a problem that was fixed, remains fixed.

The final audit report is in two parts. The first part is an Executive Summary that outlines the audit scope, findings, and recommendations at a high level. The Executive Summary is provided only to senior managers and the audit committee of the Board of Directors in compliance with the audit report distribution protocols mandated by the organization.

The second part of an audit is the Detailed Audit Report. This report is provided to the managers responsible to address the audit findings. It contains a detailed list of the findings and recommendations.

The final report is distributed carefully to ensure that it does not breach confidentiality and organizational requirements.

Visualization

In order to explain the results of the audit and the results of monitoring processes, many organizations will use graphs, tables, or other methods to help visualize the data. This may make the data more readily accessible and understandable to management.

It has been said, “A picture is worth a thousand words,” and the use of visuals in presentations can help non-technical people comprehend technical details.

Summary

Audit reports are extremely valuable means of communicating to management and highlighting areas for improvement. But they are also confidential documents that should be carefully distributed and retained.

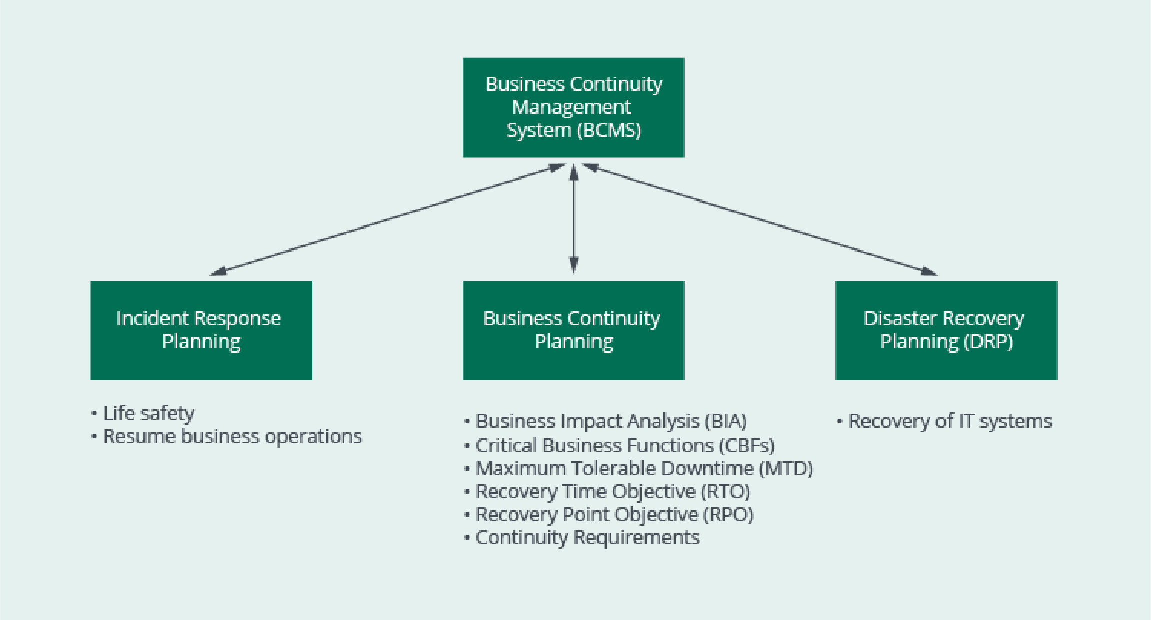
Incident Response Overview

Every organization must be prepared for incidents. Despite the best efforts of management and security to avoid or prevent problems, it is inevitable that adverse events will happen that have the potential to affect business mission or objectives. The incident response process is aimed at reducing the impact of an incident so that the organization can resume the interrupted operations as soon as possible.

The first priority of any incident is to protect life, health, and safety. When any decision related to priorities is to be made, always choose life safety first.

The secret to incident management is to be prepared. Preparation requires having a policy and a response plan that will lead the organization through the crisis. Some organizations have used the term “crisis management” to describe this process, but the term “incident” sounds somewhat better in the news media.

The relationship between the parts of business continuity management can be seen below:



Business Continuity Management System (BCMS)
Incident Response Planning
Business Continuity Planning
Disaster Recovery Planning (DRP)
• Life safety
• Resume business operations
• Business Impact Analysis (BIA)
• Critical Business Functions (CBFs)
• Maximum Tolerable Downtime (MTD)
• Recovery Time Objective (RTO)
• Recovery Point Objective (RPO)
• Continuity Requirements
• Recovery of IT systems

As can be seen, Incident Response Planning is a subset of the greater discipline of Business Continuity Management. The development of resilience and the ability to continue business operations in the face of adversity is known as a Business Continuity Management System. This is described in more detail in ISO 22301 and the Good Practice Guidelines issued by The Business Continuity Institute (thebci.org). Another organization that is a world leader in this field is Disaster Recovery Institute International (drii.org). NIST has several excellent documents that describe the components of continuity programs SP800-34r1, Contingency Planning Guide for Federal Information Systems; SP800-61r2, Computer Security Incident Handling Guide; and NIST SP800-184, Guide for Cybersecurity Event Recovery.

An event is any measurable occurrence, such as a log entry. Most events are harmless; however, if the event has the potential to disrupt business mission, then it is called an incident. Every organization must have an incident response plan that will help preserve business viability and survival.

Most incidents are minor and can be handled easily with minimal impact—a system requires a reboot, for example, but after a few minutes the system is back in operation and the incident is over. But once in a while, a major incident will interrupt business for an unacceptable length of time, and the organization cannot just follow an incident plan but must move toward business continuity. Business continuity is the process of using an alternative way to continue critical business functions that were affected by a major or long-term incident.

The Steps in Incident Management Planning

Incident management starts with planning. This allows the organization to be prepared for an incident and then to have the capability to respond effectively. While the security practitioner is not usually going to lead the incident management response effort, the practitioner's knowledge of and support for the process is important.

The exam outline for the SSCP looks at Incident Response in the following areas:

1. Discovery
2. Escalation
3. Reporting and Feedback Loops
4. Incident Response
5. Implementation of Countermeasures

These may not be the same names as the steps used by other organizations, but they will be used here as a way to step through the incident management process.

Each step has specific goals and functions that all work together to prepare for, prevent, detect, and respond to incidents in an organized, effective manner. An incident is by its very nature a time of chaos and the steps taken prior to the incident to develop a plan and to train the staff may help the organization to minimize the impact of the event and recover in a timely manner.

Discovery

The first step in incident planning is to develop a policy that declares who is responsible for the incident management function. The policy grants the authority necessary for an incident team to investigate an incident and seize equipment when necessary. The policy and incident management plan must follow the relevant laws that apply and should be coordinated with other policies, such as Human Resources and IT policies, and with Union contracts.

The Team

Incident management requires skilled individuals to handle the incident and restore operations, while also gathering the data (evidence) needed to investigate the incident and learn from it. The team should be led by a leader knowledgeable about the plan, business priorities, and legal considerations. This can require managerial and communications skills, as well as technical proficiency.

Depending on the size of the organization, the team may consist of permanent members with various skills, or it may have virtual members that can be called on when necessary. All members should have a backup in case they are not available at the time of the incident.

Having members with various skills and representing various departments is essential to ensure that the team can handle any type of incident from malware to fraud or from a natural disaster to a security breach.

Alerts

The team cannot respond if it not aware of the incident, and this is where many organizations struggle. It is common to hear of organizations that have been breached for months and not been aware of it. This requires organizations to be more diligent to detect incidents through monitoring and training.

When an alert comes in, it should always be documented. This starts the actual incident response process and ensures that a record of the incident is maintained. The challenge, however, is to determine whether the alert truly relates to a real problem (true positive) or a false alarm (false positive).

Escalation

Once an incident has been detected, the response team needs to be activated. Another department, such as a Network Operations Center (NOC), may notice the incident, and they will need to have a defined process in place to notify the incident response leader. Depending on the nature of the incident, the leader may need to escalate the incident to activate the incident response team or management.

There are several factors that affect the escalation process. In the event of a criminal incident, the organization should have an approved process to follow to notify law enforcement. This process may require the incident manager to notify a senior manager who then has the responsibility to liaise with law enforcement. A good general rule is that if the incident may be criminal in nature, the security and incident management teams should secure the scene and not do anything that could contaminate the evidence or damage the investigation.

Other considerations regarding escalation could be the size of the incident and whether it affects more than one department or system, the visibility of the incident and whether it is an incident likely to be broadcast on news media, the nature of the incident whether it is intentional or accidental, internal or external, and whether it is likely to be of a short or longer duration.

It is often said that the first step in an incident is data gathering to learn as much as possible about the incident.

Reporting and Feedback Loops (Lessons Learned)

Reporting is an important part of incident response. Reporting includes informing management and staff about the incident and may even include reporting to outside entities such as media or regulators. Open, honest, and timely communications is vital to avoid the spread of rumors or fear. Throughout the incident, management should receive reports on a regular basis.

Every incident presents the opportunity to learn. From analysis of the incident, the organization may learn how to prevent future incidents, improve detection of incidents, improve the response to the incident, and train staff to be more skilled in incident response.

Many incidents are caused by a trigger that initiates the incident; however, the root cause of the incident must be determined, not only the trigger or symptoms. Investigation of the incident may reveal predisposing conditions that led to the problem, and these must be discovered and corrected.

Feedback regarding the incident should be gathered from a review of the documentation and interviews with the staff involved. The views of all staff should be sought to ensure that there is a complete picture of what went well, what could be improved, and who provided leadership and value to the incident response team. The goal is that good actions are identified and continued, and poor actions are addressed.

It is important that the data gathering is not based on pointing blame. A fear of blame will cause people to hide issues and refuse to participate in the feedback.

Incident Response

Every organization should have a series of incident response plans prepared and ready for the various types of incidents that may occur. The plans should be of a consistent structure (the same paragraph headings and order) to facilitate reading and be readily available to staff. The plans must be followed to ensure everything is done and everyone involved knows who is doing what. Otherwise it is easy to overlook something critical or assume that a another person is doing a task when they aren't. It would be impossible to write a plan for every type of incident, but the plans provide a framework (a structure) for incident response that can be used even if there is no exact plan for a specific incident.

Incident response planning is closely linked to risk assessment and threat modeling. Plans are written to address threats, acknowledge vulnerabilities, and protect assets. The primary asset of the organization is people, and life safety is always the first priority in the plan. In the case of a fire, for example, the first step is to sound the alarm to evacuate the building before attempting to fight the fire. In the event that it was not possible to out the fire, it may be too late to sound the alarm.

By addressing risk, the incident response plan can help avoid an incident, or if it is not possible to avoid the incident, to create a level of awareness and monitoring so that the incident will be detected and responded to in a timely manner.

Once an incident is detected, the next step is to gather information about the incident. This allows the responders to determine if the incident is serious and real or just a false positive, and through that analysis to notify and escalate appropriately. This step is often known as "triage," which gathers the data needed to prioritize and classify the incident.

The next steps in incident response are to contain, analyze, and track the incident (CAT). The less that is damaged, the less needs to be repaired, so the containment step is to regain control over the incident and then to prevent it from spreading to other areas (buildings, systems, networks, etc.).

Analysis and tracking of the incident is critical to determine the source of the incident (internal or external) and to document all actions taken, including recording incoming information about the incident, decisions being made, evidence being seized, and developments in the resolution and restoration from the incident.

The incident response team then moves to the restoration phase of the incident where the focus is on restoring business operations to normal. Following an incident, the definition of normal may change since it may be impossible to actually restore the previous conditions of the system. This means that the incident will be closed off only once management has accepted the new operating environment.

Sometimes the need to get systems back into operation may conflict with the need to gather evidence and investigate the incident; however, this is an argument that the business will usually win. The most important thing for management is to resume operations even in the event that some data related to the investigation may be lost. IT is critical to ensure that all the vulnerabilities leading to the incident, such as breached passwords or unpatched systems, are resolved before turning the system back on. It would be unwise to turn the system back on only to have it compromised again.

Once an incident is over and systems are restored, the feedback phase begins. This phase is intended to learn as much as possible about the source of the incident so that controls can be enhanced or replaced, policies can be modified, procedures can be adjusted, people can be trained, and all other areas of the incident response plan improved.

Implementation of Countermeasures

There are many organizations that have never learned from previous incidents. This means they lose the opportunity to improve their resilience and incident response and are susceptible to the same incident happening again.

The lessons learned phase should lead to action where the necessary changes are implemented, monitoring improved, staff trained, and tools purchased.

There should be a schedule that proscribes the timeline for making the necessary changes and records the progress of the various projects used in implementing the changes.

Summary

Incident management is an important part of organizational resilience and survivability. Whether an organization can handle an incident effectively or not may determine the eventual level of impact of the incident and affect whether the incident is contained and eradicated or whether it spreads and causes further damage. The secret is to be prepared and have a plan, a team, and the tools necessary to respond effectively.

Information Systems Contingency Planning

The discipline of Business Continuity Management is comprised of three main divisions: Incident Response Planning, Business Continuity Planning, and Disaster Recovery Planning. In the previous section, the area of Incident Response Planning was addressed to preserve life safety and restore business operations in the event of an adverse event that could impact business mission or goals. Most incidents can be handled through an incident response plan and do not require further action, but some incidents are of the magnitude of harm or length that further steps are required to continue business functions despite the interruption. This next step is to develop Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP).

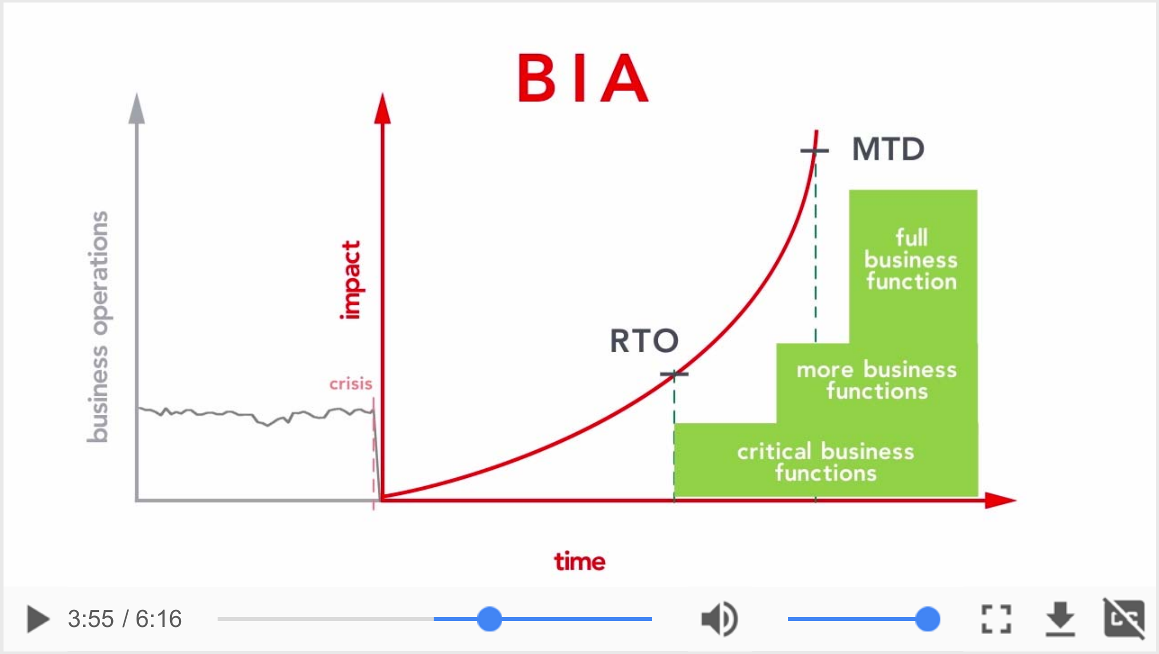
Business Continuity Planning

BCP is the discipline of maintaining the continuity of critical business functions in the event of a catastrophic event that would impact business operations for an extended period of time. It is noteworthy that BCP is NOT about keeping everything running—instead it has a focus on the critical products and services that the organization provides and ensures that those critical areas can continue to operate (although almost certainly at a reduced level of performance) until such time as the business can return to normal.

Business Continuity Planning is a project-orientated function that can be divided into five major phases:

- Project Initiation
- Business Impact Analysis (BIA)
- Selecting the Response Strategy
- Writing the Plans
- Implement, Test, and Maintain the Plans

Each of these phases will be examined in more detail.



▼ Transcript

Let's take a look at business continuity planning and the various elements of that. We know that time goes on, and as time goes on the business is running at a normal level of operation until, for example, maybe one day, we have a crisis. As a result of that crisis our level of operation has dropped off to nothing, the business is not operating. Through BIA, we calculate what is the level of impact of that outage on the business. In both, of course, quantitative manners as well as qualitative. If the business is not operating, we know that there's going to be a financial or a quantitative impact as well as an impact on customer confidence, employee moral, as well as of course, reputation of the business. So we do this analysis of the impact of this outage on the business, something we call BIA. And in BIA, we are looking at the impact of this outage over the time period, slightly different than risk assessment. Risk assessment said what would be the impact according to the likelihood or probability of that event. We know that when we calculate this, we have to determine the timescale that's being used. Is time being measured in days, weeks, or maybe even miniature hours. Depending on the type of business we're in the region, as well as of course, any other type of legal requirements we could have. There's also, of course impact depending on the type of system it is. Some systems, the outage could be in days and would not really cost us very much. Whereas other times, at a hospital for example an outage, even of minutes could be life threatening. We determined what was our Maximum Tolerable Downtime. What's the maximum allowable level of outage we could suffer before the business's very viability or its ability to recover would be impacted? This was also known as Maximum Allowable Downtime or Maximum Tolerable Period of Disruption. It's the point in time in which we may not be able to recover because of the impact of that outage. Knowing that is important because now we can determine what is our desired point of recovery, and this is something we will call our recovery time objective. We set an objective for when we want to be able to recover, at which point in time, which must be less than our Maximum Tolerable Downtime. Normally when we recover, we will recover critical business functions first. We won't recover everything, we will recover that part of the business which is essential for our customers and operation. Over time, we may recover other parts as well until someday, we can restore to normal knowing that normal may not be the same as it was before, in the case of a catastrophic fire for example. So we've sat out what we will recover and at what point in time. But there's something else we have to know as well. In the time period preceding the crisis we were doing data backups and those data backups were important so that we had the data necessary to be able to recover. When we recover, we will normally be then, required to use our most recent backup of our data. The problem with that is that all of the data from the time of that backup until the time of the crisis could then be lost data. Depending on the type of system, I may not be able to recover any transactions or processes that happened between the time of the backup and the time of the failure. This is where we have to get to know what is our recovery point. Our Data Recovery Point will usually be determined by the frequency of our backups and the type of backup we use. And we've set a Recovery Point Objective. The Recovery Point Objective, or RPO is where we determine what is the frequency and type of backup we use for our data to ensure that we don't lose more data than we are willing to lose based on the value of our data. The volatility of the data, how much does it change. So in some cases, my data may not change much from one day to the next and doing a daily or weekly backup could be good enough. In other cases, we could process millions of dollars worth of transactions within a few minutes and we would have to have a data recovery based on mirroring or some other type of real time data recovery operation. In all of this, we are able now to put together the critical pieces necessary for a business continuity plan.

Project Initiation

A Business Continuity Project is like any other project in that it requires careful project management. Like any other project, it is important to follow good project management principles to improve the likelihood of project success. This includes setting out the scope of the project, resources, timelines, deliverables, and authority.

A BCP project must have support of senior management to be successful. The project team will have to gather information from many departments and individuals to develop the plans, and this requires access to those departments and to the record of past incidents. Many managers may see BCP as an unnecessary intrusion on their time and be unwilling to support the project unless that support is mandated by senior management. After all, BCP is all about preparing for events that you hope will never happen—so the pressure of today’s issues is a much higher priority for most managers.

Scope must also be determined in this phase. Scope is often based on examining the continuity of a product or service and how to keep that business function operating; however, scope may also be based on a geographic location where the BCP will be, based on an incident that affects one branch office or other geographic location.

A BCP project should never be viewed as a one-time effort where the strategy is to write a plan and then just save it for use if necessary. Instead, the plan needs to be developed as a long-term project that allocates the resources (money, personnel, software) to write the initial plan and then provide for an annual budget to maintain and test the plan.

A BCP project often starts with enthusiasm and then fades into endless discussion and complacency. This is why it needs careful project management, definite timelines, and skilled leadership. The project must be led by a person that has excellent communications skills and leadership ability. This person must coordinate the use of time and resources to maintain project focus and timelines. Otherwise support for the project will quickly wane.

Business Impact Analysis (BIA)

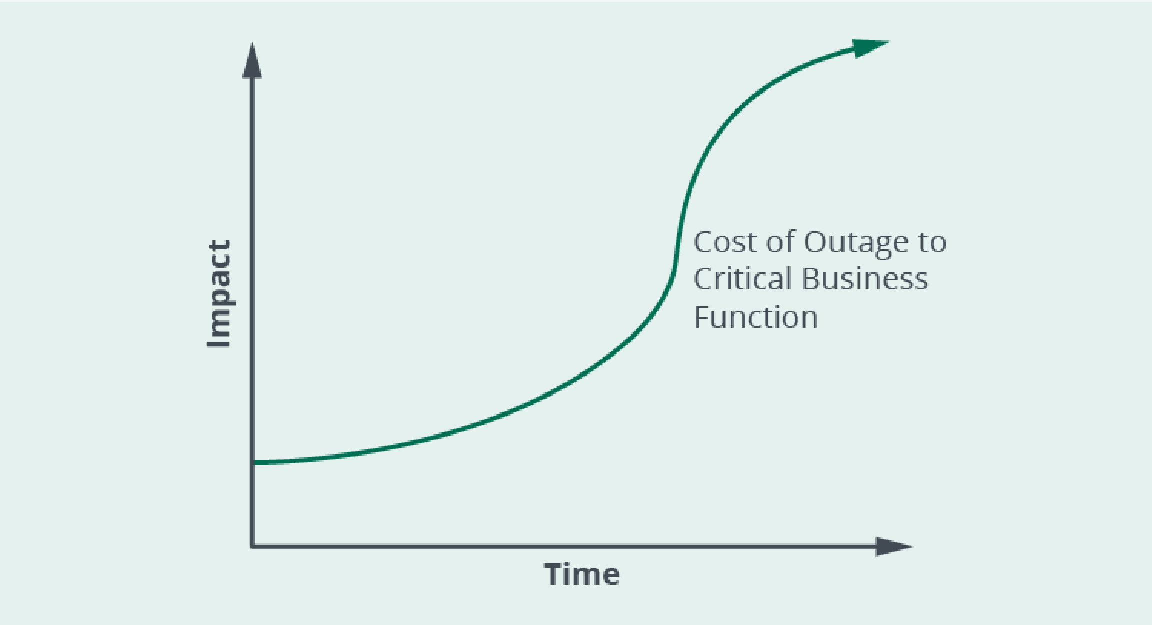
Business Impact Analysis (BIA) is the heart of the BCP project effort. BIA identifies the critical business functions, the critical timelines, and the resources necessary to support those business functions. The very name BIA indicates the core focus of this phase—the Analysis of the Impact of an outage on the Business (BIA). BIA is based on the business impact not just on the impact to a supporting function such as IT.

BIA is based on two factors, time and impact. Impact is measured through both qualitative and quantitative measures related to the length of the interruption to the business function. If a call center is unable to respond to customer calls because their supporting information system is down, then the impact will often be related to the length of the outage as well as the loss incurred due to the outage. The longer the system is down, the longer the call center cannot operate and the greater the impact. From this example, we can see that the true impact from the loss of an information system is based on the impact to the business, not just on the cost to the IT department.

Calculating impact is not easy since the impact can vary widely depending on many factors. An outage at the end of the day may have less impact than an outage at the beginning of the day, and the impact may be affected by how widely known the incident is—in other words, does the incident make it to the newspapers.

Impact can be determined using quantitative methods where the financial cost of the outage is measured. For example, a call center may generate a certain amount of revenue per hour, and the cost may be simple to estimate based on how long the systems are out of service. But this calculation should also consider other factors such as overtime costs to catch up on work that could not be done during the outage, the cost related to breach of contract and service level agreements, or regulatory fines for not meeting expected service and security levels.

Qualitative impact also considers the impact on customer confidence, reputation, employee morale, and other non-quantitative factors. A proper impact analysis should consider both quantitative and qualitative factors.



As can be seen in this image, the degree of impact may change over time. The rate of change will often increase over time.

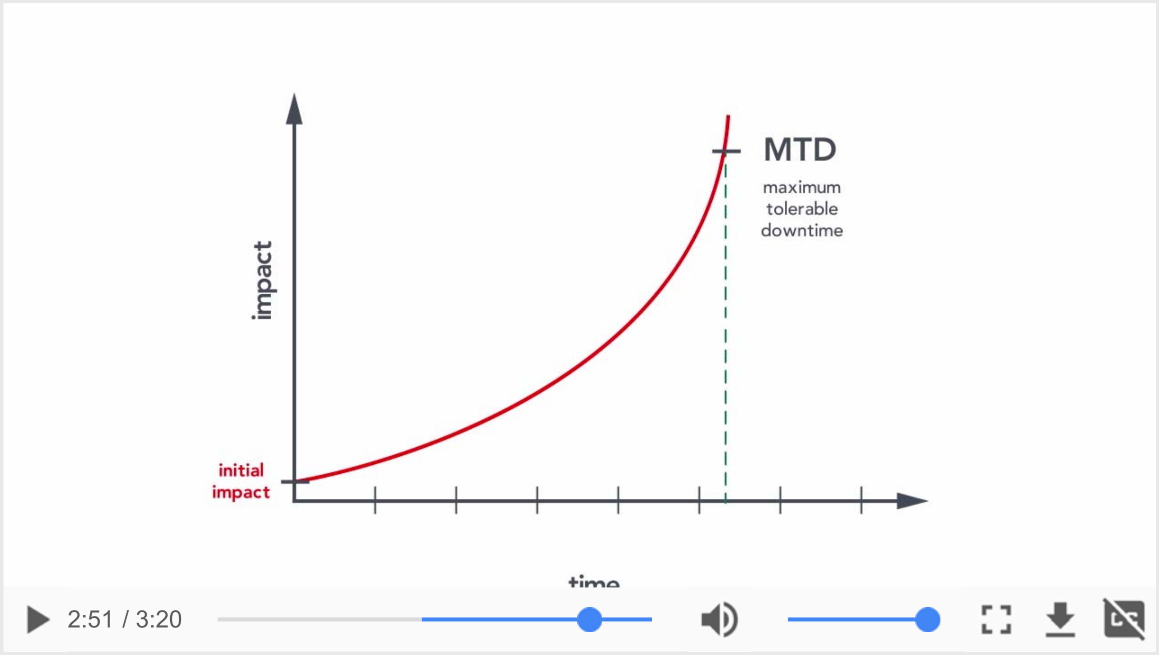
The art and skill of BIA is to learn what the impact levels would be according to each product, service, geographic location, or information system. This varies widely from one system to another. The timescale is also important. Some systems may have a high level of impact within minutes, while another system may have limited impact for several hours or even days.

The BIA effort must identify which systems are critical to the organization and which ones aren't. For example, an outage of internal audit would probably have very limited impact for several weeks, while an outage of the website for an e-commerce company would have a high level of impact within minutes.

This effort identifies the products or services that must be recovered first in the event of a major crisis, and those areas that can wait until later for recovery.

Risk assessment is also a partner to BIA, they are not the same but they support one another. Risk assessment examines impact and likelihood whereas BIA examines impact over time. A BCP effort should address the items listed in the risk assessment and plan for the recovery of those business functions in the event that a risk event does occur. The BIA should also be prepared to address the types of incidents the organization has been subject to in the past.

At some point in time, if an organization has not been able to recover a business function from an outage, the business will cease operations. This is the point at which the very survival of the organization is at stake. This time would indicate the Maximum Tolerable Downtime (MTD). Depending on the source document used, this has also been called the Maximum Tolerable Period of Disruption (MTPD) or Maximum Allowable Downtime (MAD).



▼ Transcript

Let's take a look at Business Impact Analysis. It's important to remember that Business Impact Analysis is an analysis of the level of impact on the business. This is important to remember. We're looking at the impact on business, not just on the impact on information technology systems. This is an important calculation we need in order to be able to do business continuity and disaster recovery planning. With BIA, we're going to look at what is the level of impact of some type of an outage over the time period, or duration, of that outage. Say, for example, a critical system was out of service. A cable is cut. How would that impact the business over the duration or time period that that outage remains? We can calculate impact, both in, well, quantitative values, for example money, or qualitative values, things like reputation, customer confidence, morale of the employees. We say that there's an initial level of impact once there has been an outage. And that impact will usually increase over time. Not just straight linear, quite often the level of impact will increase exponentially even, as the time period of that outage remains. We'll reach a certain point in time where we could say the level of impact is so great that the very viability of the business could be threatened. The business would not be able to recover. That is what we'll call our Maximum Tolerable Downtime. If our outage has remained for that length of time, we would not be able to recover. In time's past, it has been known as Maximum Allowable Downtime, and sometimes called The Maximum Tolerable Period of Disruption. We want to know what is the time period that we will be at that point? We have to write a business continuity plan that ensures we'd be back in business well before we reach that point of no return. An important calculation, however, is to know what is the time scale? This time scale can be very different depending on the business, the system, the department, the region of the world, and can be measured in anything from days, in some cases, to even minutes, if we were, for example, a hospital. We need to know and be able to determine through our analysis what would be the impact on business operations of various types of outages we could face.

Recovery Time Objective (RTO)

The cost to recover from an outage is often the inverse to the length of the outage. In other words, the cost to provide continuous service through redundancy is expensive, but the cost to recover a few hours or days later is less expensive. The data gathered during the BIA process can be used to justify the decision to be made in the next phase of the project on what type of business continuity solution is best for each product or service provided by the organization

The intent of developing a Business Continuity Plan (BCP) is to develop a road map and strategy that can lead the organization through the steps and activities necessary to continue business operations affected by the outage. The plan has a goal of resuming the identified critical business functions (CBFs) within a time frame known as the Recovery Time Objective (RTO). The RTO is set by management based on the impact of an outage over time and the cost of the various recovery options. The RTO must always be less than the MTD.

Recovery Point Objective (RPO)

The Recovery Point Objective is based on the maximum amount of data an organization can lose in the event of a loss of information systems. If an information system is interrupted by a failure, the organization may have to rebuild the system from backups. This means that the state or condition of the information system, once recovered and ready to resume operations, will be dependent on how current the backups are. If the backups are done once a week on a Saturday evening, for example, and the system crashes on a Thursday due to hard drive failure, then any patches, configuration changes, or transactions that have been done during the week would be lost. The organization must determine whether the loss of four or five days' worth of data is acceptable or not. The impact of the loss of data is affected by the amount of change in the data, the value of the data, regulations surrounding data retention, and the time it would take to rebuild or restore data if at all possible.

To avoid the loss of an unacceptable amount of data, the organization would need to conduct backups at a more frequent basis. This may be done by backing up information systems daily, hourly, or even mirroring data to avoid data loss. A full backup may be conducted every weekend, for example, and then an incremental backup done daily to record the changes that have been made during that day. Another option is to do a daily differential backup that would record all changes since the last full backup. Backups should be protected from disclosure through encryption and from errors through the use of hash functions and proper handling.

If backups are stored off-site, then ensure the method of transport is secure and that the encryption keys would be available when required. The off-site location should be secure and available so that the backups can be retrieved when required.

The type of backup chosen is also important since the time taken to recover from a tape backup may mean that the organization cannot recover an information system in time to meet the RTO. Backup media also deteriorates over time and use, so the number of times a backup media (tape, solid state drive, etc.) has been used and the age of the media should be tracked to ensure the organization is not relying on backups already past life expectancy (often expressed as Mean Time Between Failure or MTBF).

Continuity Recovery Requirements

The other important objective of the BIA effort is to determine the Continuity Recovery Requirements for critical business functions. These can usually be listed as:

- Personnel
- Equipment
- Data
- Facilities
- Supply chain

Documenting these requirements will help in the writing of the plan. For many departments, the level of service provided during a recovery will be at a lower level than normal operations. This may mean the department can operate at a reduced level of staff. The number of staff and the skills required of staff need to be identified so that the appropriate staff is on board during the first phases of the recovery.

The data gathered during the BIA is often obtained through interviews with managers, users, and IT administrators and a review of process documentation, previous incidents, audits, and observation. The more thorough and accurate the data gathering, the more likely the results of the BIA will be correct and aligned with business priorities.

A side benefit of conducting a BIA is that risks may be identified that could be mitigated and help prevent a future outage. The BIA may identify single points of failure, outdated processes or equipment, or a weakness in a business process that can be addressed.

The results of the BIA are then presented to management for review and feedback. Management should ensure that the critical business functions are correctly identified and that the timelines for those functions are correct. Management will also review the proposed RTO and RPOs to ensure that they are in line with organizational objectives and priorities.

Once management has approved the BIA, the BCP project is ready to move into the next phase.

Recovery Strategy Selection

The BCP project team now has to determine which recovery strategy is best for the organization. This is dependent on what options are available since sometimes there are few viable options. An organization that uses unique equipment or is located in a remote location may have few continuity options available, whereas a more traditional organization that operates in a large city with commonly available systems and equipment may have a number of possible recovery alternatives.

The first step is to determine how to recover critical business functions within the RTO. In the event of a fire in a facility, some functions may be provided through an office in another region, and the organization can just support the impacted region by increasing staff or hours of operation at the other location. The organization may choose to outsource some functions to a third party. This is often done with areas that are simple to outsource such as call center operations, payroll, and manufacturing. In some cases, the organization will suspend less critical operations, such as training, and use the office space and equipment in the training rooms for supporting an impacted critical business function (sometimes called displacement). Sometimes the organization may even be able to support a critical business function through reverting to a manual process for a short time. Non-critical business functions will usually be suspended until the CBFs are in operation. Depending on the duration of the outage, these less critical functions may be recovered gradually as resources permit.

Disaster Recovery Planning (DRP) - Recovery of Information Technology

The recovery of a business function may be done independently of the recovery of IT services. As seen above, the organization may be able to recover a CBF without IT; however, the recovery of IT is often crucial to the recovery and sustainment of business operations. The recovery of IT services is known as Disaster Recovery Planning (DRP).

DRP is the discipline of recovering IT services that support the business operations. The IT requirements were identified in the BIA phase as equipment, personnel, and data necessary to support business operations. The DRP team then considers how to support and meet the BCP team through the development of a strategy that will provide for the necessary IT services within the required time frames. There are several options available for the recovery of IT services including:

- Multiple Processing Centers (MPCs)
- Mirrored Site
- Commercial Hot Site or Mobile Site
- Warm Site
- Cold Site

Multiple Processing Centers

An organization that has a requirement for continuous operations may choose to operate more than one data center in parallel. This would mean that an outage at one location would not result in the total loss of system functionality. Obviously, this is a very expensive operation since it requires almost full duplication of personnel, equipment, data, and networks. The advantage is that systems can run in a continuous mode and any crisis should not interrupt service.

Mirrored Sites

This recovery strategy is only slightly less expensive than multiple processing centers. The organization has an alternate site for data processing that is a mirror of the primary site and kept up to date with data changes and operations; however, the site is not functional and would require a few minutes of outage before being completely operational. This is a good solution where an outage cannot last for more than a few minutes.

Commercial Hot Site

These sites were the traditional form of disaster recovery for decades. The idea is that there are several of these sites available from various vendors that are fully equipped data centers and available for rapid usage in the event of the loss of IT services by an organization. These sites can usually be operational within four to six hours, and several companies may subscribe the services of a hot site. This requires some attention to ensure the site would be available in the event of a major regional disaster. This is an expensive option but less costly than multiple processing centers.

One of the options available for most organizations today is migration to the cloud. In the event that an organization loses its core server rooms or data center, the organization may select to move to a cloud provider as a permanent option.

For organizations already on the cloud, there is still the need to ensure that IT services will be available in the event of a disruption by the cloud service provider. The cloud service provider is operating a data center and subject to system and network failure like anyone else. Therefore, an organization using a cloud service provider should also ensure they have terms in the contract to provide data and system availability in the event of a failure on the systems of the cloud service provider.

Mobile sites used to be more popular than they are today since they have often been replaced by the Cloud. A mobile site is a server farm in a truck that can be shipped (driven) to a client location on demand. This is a good option when a fire or water damage may have affected the server room of an organization. The mobile site has racks of equipment, network capability (often satellite), workspace, and electrical power (the diesel of the truck) so that it can be onsite to provide IT infrastructure in a matter of hours (depending on how far the truck has to travel).

Warm Site

A warm site is a partially equipped server room or data center that can be brought on line in days. Often this is the backup site so the organization has the data onsite, some equipment, and networking capability, but it is lacking some of the more expensive equipment needed to support all required business operations. This site is often supported through agreements with vendors to ship in the necessary equipment in the event it must be built out to full operational status.

Cold Site

A cold site is a facility that has the networking capability, power, and air conditioning required to operate a data center but no computer equipment or data. This form of recovery would often take weeks to bring online, but it may be a good option for a staged recovery where the organization moves their data processing to a commercial hot site at the time of the initial failure and then relocates to the cold site once it has been built out.

In this phase of BCP, the project team must select the best option for recovery based on cost, availability, time frames, and management preference.

Once the recovery strategies for business operations and for IT (DRP) have been selected, the project moves onto the next phase, writing the plan.

Writing the Plan

At this point, all of the data needed to write business continuity plans and disaster recovery plans has been collected and the recovery strategy approved by management. This allows the BCP project team to write the plans to recover business operations within the RTO. BCP and DRP are action-orientated and should list the steps necessary to recover operations. There may be many different plans depending on the type of incident that occurs. Each plan should list the steps and activities necessary to resume operations. Each step should be assigned to the appropriate person (including a deputy) to direct the team through the steps and checklists that will ensure a step is not missed or overlooked.

The plans should be written as modules so that they can be updated and replaced as necessary without rewriting the entire plan. The plan(s) may be stored on paper or electronically as long as they would be available when required by the recovery teams.

Restoration

The ultimate goal of Incident Response Planning, Business Continuity Planning, and Disaster Recovery Planning is to build an organization resilient to failure and avoid a crisis whenever possible and also to detect and respond to any crisis in a timely and effective manner so there is minimal impact of a short duration that enables the business to restore normal operations in a minimal amount of time.

In the event of a crisis, the most important business functions are recovered first and then others may be recovered later. But the goal is to get back to normal even though normal may be quite different from what normal was before the crisis. A fire may result in permanent relocation to another facility, so the end of the crisis is relocation and normal operations at the new normal location. The crisis ends once the business is back to normal operating status.

When the business restores to normal, it usually will restore the least critical services first. This is the opposite of recovery, which recovers the most critical services first. Restoring the least critical services allows the organization to test the networks, migration plan, and other elements of the restoration to make sure everything is working correctly before jeopardizing critical business processes through their restoration.

Testing, Maintenance, and Implementation of the Plans

BC and DR plans quickly become outdated as the business changes, as personnel changes, and as technology is replaced. This requires an ongoing effort to keep the plans up to date.

Testing the plans provides two primary benefits—the training of the personnel that will be members of the recovery teams in the event of a crisis, and the discovery of any gaps or problems in the plans that should be corrected before a real crisis occurs.

There are several forms of testing that are used to validate BC and DR plans including:

- Deskcheck
- Tabletop exercises (structured walkthroughs)
- Simulations
- Parallel Test
- Full interruption

A deskcheck should be done at least annually by each manager to review the plans for their department and ensure the plans are still current. This test is the most basic and can identify if critical systems, operations, or personnel have changed.

A structure walkthrough requires the personnel from the teams to meet and step through the plan around a boardroom table (hence the name tabletop exercise). The test will address a certain type of event, and each member of the teams would state their responsibilities if such a crisis did occur. It helps each team member to know how their job interacts with the other team members and see if any areas were missed in the plan.

A simulation is where a simulated crisis is enacted such as pulling a fire alarm and evacuating the building, or requiring IT staff to rebuild a server. The test reviews that personnel know how to react to the crisis and follow the plan. This type of test can discover whether the plan's timelines are realistic and whether some critical steps in the plan have been overlooked.

A parallel test can be conducted when the organization has access to a commercial hot site. The organization can load all their data on the systems of the hot site and then run those systems in parallel with production for a day. This ensures the backups are complete, the systems are compatible, access permissions are correct, and the ability to recover within timelines is feasible.

A full interruption test is only conducted with the approval of senior management. This type of test may be required by law or regulation for systems that support critical infrastructure. These tests run a high risk since they may cause business interruption. In a full interruption test, the primary systems are disabled, and the backup systems must come online and operational within the critical timelines. This is the type of test that can only be done when the organization has multiple processing centers or redundant equipment.

Tests should be scheduled for all areas of the plans and to train personnel, including deputies. Each test should be reviewed to see where the plans could be improved. The plans will change over time as business priorities change, and this requires the updating of the plan as well as version control. Everyone should be accessing the same plan and know what systems or processes are most important for recovery.

The results of any crisis, test, or audit should be reviewed to see if the plans need updating.

Summary

The ability of an organization to prepare for an incident and have plans in place to recover following an incident will make a difference in the overall impact of an incident. The organization should have incident response, business continuity, and disaster recovery plans in place and ensure staff is trained and knowledgeable about what to do in a crisis.

Understand and Support Forensics Investigations Overview

The purpose of an information security program is to protect the organization from a breach or failure that would impact the goals and mission of the organization. The strategy is interpreted through policies, procedures, baselines, and standards to set out the expected behaviors of staff and the mechanisms in place to prevent, detect, and respond to incidents. However, despite the best strategy and the deployment of controls, incidents will still occur that require an investigation of the incident and the personnel involved.

An incident that involves personnel may be the result of intentional or accidental actions. The personnel involved may be internal, external, or a combination of both. The role of the security practitioner is to support the investigation through securing evidence, providing log data, examining network traffic, or doing a forensic investigation of storage media (hard drives, USB drives, SD cards, etc.). In some cases, the security practitioner may even be involved in doing reverse engineering of malware to determine the nature of, and infection mechanisms used by, the malware.

When a security incident occurs, the security practitioner should follow the incident response procedures outlined in the incident response plan. This begins with documenting the incident, determining the type of incident, and notifying or escalating the incident as per the plan.

In the event that an incident appears to be criminal in nature, the security practitioner is best advised to secure the scene, notify management according to the defined procedures, and take no further action unless directed by law enforcement or management. To undertake further action may damage the integrity of the scene and lead to the loss of acceptability of the evidence.

The first step in any investigation is to start the documentation. Each potential incident should be documented so that it can be reviewed and analyzed following the incident. If the security practitioner needs to secure evidence needed to support the investigation, the evidence must be collected in a lawful manner. It is not acceptable for a security practitioner to use illegal methods to gather data. The evidence should also be protected through the chain of custody through the evidence life cycle. The chain of custody is an unbroken, documented record of what has happened to the evidence from the time it was first seized through its analysis, transportation, storage, and reporting until such time as it is returned to its rightful owner or destroyed. The evidence custodian maintains the chain of custody. As evidence is seized, it is passed to the custodian to record who seized the evidence, when, how it was protected, and where the seizure took place. The chain of custody can protect the integrity and acceptability of the evidence to demonstrate that no unauthorized changes have happened to the evidence and that unauthorized personnel did not access it.

A lot of evidence, such as logs, may only be available for a short time before it is overwritten. This requires the investigators to secure the logs and other evidence that may otherwise be lost as quickly as possible once an incident is reported.

Digital evidence is easily contaminated, and the very act of viewing the evidence may change its state. Therefore, the seizure of digital evidence should take appropriate steps to maintain the integrity of the evidence. When a hard drive must be seized, the investigator must take two bit level images of the drive using a write protect diode to prevent the writing of any information back onto the source (original) drive. The original drive should be run through two hash functions to indicate whether the data on the drives has been altered. Using two different hash functions increases the trust in the integrity of the evidence. The data on the original should be copied onto clean, unused destination drives. One destination drive will be used as a library copy and the other destination drive as a control copy. The original drive should be sealed in an evidence bag with tamper-proof tape, logged, and stored securely. The use of bit level images will copy all data on the source drive including deleted files, virtual memory, and other artifacts necessary for the investigation.

Real, direct evidence is always better than copies or evidence provided by a third party. If the investigator did not collect the evidence themselves, they may not be able to validate that the evidence is complete and unaltered.

Securing the Scene

Once the scene of an investigation has been altered, it may be impossible to verify the integrity of the investigation. The investigators must protect the scene from improper alteration and prevent the contamination of the scene as much as possible. It may be impossible not to change the scene since an investigator cannot seize a laptop or desktop that is turned on without making some changes to its state.

Once an incident has been reported to the investigators, the investigators should review whether the reported incident is covered by any relevant policies or laws and whether the investigative team has the authority to conduct the investigation.

The first step the investigator should take when approaching the scene is to document the current state or condition of the scene. This includes whether the laptop is turned on, what is on the screen, what is connected to the laptop, who is at the scene, and when and where the investigation is conducted.

In some cases, the investigative team may call on outside experts to assist in the investigation. This requires contractual language to address the confidentiality of the investigation and responsibilities for the outside experts regarding disclosure and reporting. Outside experts could include fraud investigators, expert witnesses, forensic investigators and interviewers.

Legal and Privacy Concerns

Security practitioners must be careful not to exceed their levels of authority or responsibility. Most security practitioners do not have the credentials of law enforcement and their actual level of authority is very limited. They cannot trample the rights of another person or violate the laws of the country. This includes the challenge of network or system monitoring. In many cases a security practitioner only has the right to monitor activity when directly authorized by management and in support of an approved investigation. Different countries have different laws regarding data surveillance and monitoring, and the security team must be familiar with those laws. This is further complicated by labor laws, union contracts, or human resources policies that must be respected. The security practitioner is only authorized to conduct investigations according to the mandate of management.

Monitoring network traffic, for example, may be subject to privacy laws that restrict the investigator from using network data for anything other than statistical purposes.

Data Privacy and Transborder Controls

Many countries have regulations in place to protect the privacy of their citizens. This requires organizations to ensure they are not transferring data to another country in violation of privacy laws. This is especially complicated when using the services of a cloud provider that may be accessing data from, or backing up data to, another country.

Interviewing

One of the most important ways to gather information during an investigation is to interview the personnel that may have knowledge of the incident. This would include interviewing managers, witnesses, co-workers, suspects, and IT administrators. Interviews must be conducted in a legal manner without intimidation or threats. The purpose of the interview is to gather information that can be used in the investigation, so the goal of the investigator is to get the person being interviewed to talk openly. Interviews must never be conducted alone but rather in the presence of at least one other observer. If possible, the interview should be recorded. An ideal interview room is a sterile environment that provides a minimal level of distraction and seats all parties in similar chairs without the perception of barriers or dominance.

Summary

Investigations are one of the most difficult parts of a security practitioner's job. Since the impact of an investigation may lead to a person losing their job, facing disciplinary action, or, in a worst-case scenario, facing criminal charges; the investigators must be extremely careful to be honest, thorough, skillful, and legal in their conduct of the investigation.