



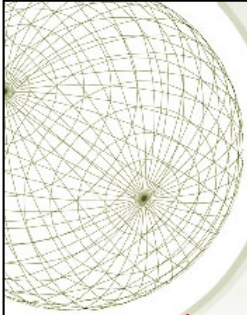
Fundamental Concepts of Data Security

Business Continuity

1

Comprehensive approach to business continuity plan

- Prevention: risk management plan (this lecture) – what to do to prevent incidents
- Preparedness: business impact analysis – if incidents do happen, what would be the impact
- Response: incident response plan – what to do when incidents happen
- Recovery: recovery plan – how to recover after an incident/disaster



COMMONWEALTH OF AUSTRALIA

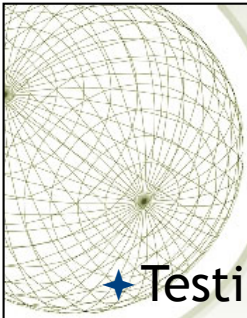
Copyright Regulation 1969

WARNING

This material has been copied and communicated to you by
or on behalf of Curtin University of Technology pursuant
to Part VB of the Copyright Act 1968 (the Act)

The material in this communication may be subject to
copyright under the Act. Any further copying or
communication of this material by you may be the
subject of copyright protection under the Act.

Do not remove this notice



Testing

- ★ Testing a business continuity plan is crucial for the success of the plan.
- ★ The test is conducted to ensure that the plan is effective in case of all eventualities.

3

The BCP should be tested regularly, because environments continually change. Interestingly, many organizations are moving away from the concept of “testing” because a test naturally leads to a pass or fail score, and in the end, that type of score is not very productive. Instead, many organizations are adopting the concept of exercises, which appear to be less stressful, better focused, and ultimately more productive. Each time the plan is exercised or tested, improvements and efficiencies are generally uncovered, yielding better and better results over time. The responsibility of establishing periodic exercises and the maintenance of the plan should be assigned to a specific person or persons who will have overall ownership responsibilities for the business continuity initiatives within the organization.

As noted earlier, the maintenance of the plan should be incorporated into change management procedures. That way, any changes in the environment are reflected in the plan itself.

Written exercise plans should be developed that will test for specific weaknesses in the overall disaster recovery plan. The first exercise should not include all employees, but rather a small group of people here and there until each learns his or her responsibilities. Then, larger drills can take place so overall operations will not be negatively affected.

The people carrying out these drills should expect problems and mistakes. This is why they are having the drills in the first place. A company would rather have employees make mistakes during a drill so they can learn from them and perform their tasks more effectively than during a real disaster.



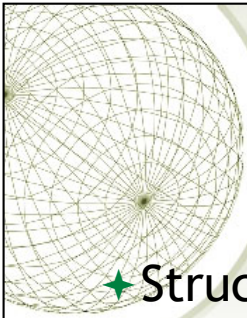
Testing

- ★ A sound BCP should be complete and focused.
 - ★ Should be manned by properly trained and competent personnel.
 - ★ Requires close coordination with external vendors.
 - ★ Should have capability of backup site to conduct prescribed processing with the capacity to retrieve vital records along with the configuration of equipment which should be relocated to the recovery site.



Testing

- ★ The BCP tests should be conducted during the slack period.
- ★ It is important that realistic prime time conditions be simulated.
 - ★ even if the BCP test is conducted during off-peak hours.



Testing Methods

- ✦ Structured walk-through test
 - ✦ *Let's get in a room and talk about this.*
- ✦ Simulation test
 - ✦ *Everyone take your places. Okay, action!*
- ✦ Parallel test
 - ✦ *Let's do a little processing here and a little processing there.*
- ✦ Full-scale test
 - ✦ *Shut down and move out!*

6

Structured Walk-Through Test

In this test, representatives from each department or functional area come together and go over the plan to ensure its accuracy. The group reviews the objectives of the plan; discusses the scope and assumptions of the plan; reviews the organization and reporting structure; and evaluates the testing, maintenance, and training requirements described. This gives the people responsible for making sure a disaster recovery happens effectively and efficiently a chance to review what has been decided upon and what is expected of them.

The group walks through different scenarios of the plan from beginning to end to make sure nothing was left out. This also raises the awareness of team members about the recovery procedures.

Simulation Test

This type of test takes a lot more planning and people. In this situation, all employees who participate in operational and support functions, or their representatives, come together to practice executing the disaster recovery plan based on a specific scenario. The scenario is used to test the reaction of each operational and support representative. Again, this is done to ensure specific steps were not left out and that certain threats were not overlooked. It raises the awareness of the people involved.

The drill includes only those materials that will be available in an actual disaster to portray a more realistic environment. The simulation test continues up to the point of actual relocation to an offsite facility and actual shipment of replacement equipment.

Parallel Test

A parallel test is done to ensure that the specific systems can actually perform adequately at the alternate offsite facility. Some systems are moved to the alternate site and

processing takes place. The results are compared with the regular processing that is done at the original site. This points out any necessary tweaking or reconfiguring.

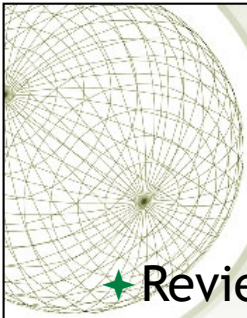
Full-Interruption Test

This type of test is the most intrusive to regular operations and business productivity. The original site is actually shut down, and processing takes place at the alternate site.

The recovery team fulfills its obligations in preparing the systems and environment for the alternate site. All processing is done only on devices at the alternate offsite facility.

This is a full-blown drill that takes a lot of planning and coordination, but it can reveal many holes in the plan that need to be fixed before an actual disaster hits. Full-interruption

tests should be performed only after all other types of tests have been successful. They are the most risky and can impact the business in very serious and devastating ways if not managed properly; therefore, senior management approval needs to be obtained prior to performing full-interruption tests.



BCP Maintenance

- ★ Review and maintenance
- ★ Integrate into change control process
- ★ Update plan
- ★ Distribute after updating

7

Why maintenance? Unfortunately, the various plans that have been covered in this chapter can become quickly out of date. An out-of-date BCP may provide a company with a false sense of security, which could be devastating if and when a disaster actually takes place. The main reasons plans become outdated include the following:

- The business continuity process is not integrated into the change management process.
- Changes occur to the infrastructure and environment.
- Reorganization of the company, layoffs, or mergers occur.
- Changes in hardware, software, and applications occur.
- After the plan is constructed, people feel their job is done.
- Personnel turn over.
- Large plans take a lot of work to maintain.
- Plans do not have a direct line to profitability.

Integrate into change control process:

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operation/Maintenance phase of the SDLC, information systems undergo frequent changes because of shifting

business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the ISCP be reviewed and updated regularly as part of the organization's change management process to ensure that new information is documented and contingency measures are revised if required.

Update:

As a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews. The plans for moderate- or high-impact systems should be reviewed more often. At a minimum, plan reviews should focus on the following elements:

- Operational requirements;
- Security requirements;
- Technical procedures;
- Hardware, software, and other equipment (types, specifications, and amount);
- Names and contact information of team members;
- Names and contact information of vendors, including alternate and offsite vendor POCs;
- Alternate and offsite facility requirements; and
- Vital records (electronic and hardcopy).

Organizations can keep the plan updated by taking the following actions:

- Make business continuity a part of every business decision.
- Insert the maintenance responsibilities into job descriptions.
- Include maintenance in personnel evaluations.
- Perform internal audits that include disaster recovery and continuity documentation and procedures.
- Perform regular drills that use the plan.
- Integrate the BCP into the current change management process.
- Incorporate lessons learned from actual incidents into the plan.

Distribution:

Because the ISCP contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled. Typically, copies of the plan are provided to recovery personnel for storage. A copy should also be stored at the alternate site and with the backup media. Storing a copy of the plan at the alternate site ensures its availability and good condition in the event local plan copies cannot be accessed because of disaster. The ISCP

Coordinator should maintain a record of copies of the plan and to whom they were distributed.



Incident Response

- ★ Computer security incident
 - ★ Unauthorized or unlawful attack against information asset (AIC)
 - ★ Occurred/completed
 - ★ Usually less significant than disaster
- ★ Incident response (IR)
 - ★ More reactive than proactive
 - ★ Plan for, detect, and correct impact
 - ★ Phases: planning, detection, reaction, recovery, review

8

What is an incident? As stated earlier, an incident is an attack against an information asset that poses a clear threat to the confidentiality, integrity, or availability of

information resources. If an action that threatens information occurs and is completed, the action is classified as an incident. For purposes of this discussion, however, attacks are classified as incidents if they have the following characteristics:

- They are directed against information assets.
- They have a realistic chance of success.
- They could threaten the confidentiality, integrity, or availability of information resources.

Examples

- Unauthorised/accidental disclosure of sensitive information
- Theft/loss of information
- Data exfiltration
- Unauthorised access/modification of information
- Privilege escalation attacks
- System malfunction (kernel panic, crashes, irresponsible) due to virus/malware, or unauthorised applications

- System memory outage
- Network unavailability

NIST further categorises incidents in terms of six attack vectors

- External/removable media (executed from media)
- Attrition (i.e. brute force methods)
- Web-based attacks
- Email attacks
- Improper usage
- Loss or theft
- Others

Incident response (IR) is therefore the set of activities taken to plan for, detect, and correct the impact of an incident on information assets. Prevention is purposefully omitted, as this

activity is more a function of information security in general than of incident response. In other words, IR is more reactive than proactive, with the exception of the planning that

must occur to prepare the IR teams to be ready to react to an incident. IR generally consists of the following phases:

1. Planning
2. Detection
3. Reaction
4. Recovery
5. Post-incident review

SAN describes six (6) phases instead:

1. Preparation (i.e. planning)
2. Identification (i.e. detection)
3. Containment (part of reaction)
4. Eradication (part of reaction)
5. Recovery
6. Lessons learnt (documenting/report/discussion)



IR Planning

- ✦ Preparation work is KEY to successful incident handling
- ✦ Unlikely to find multiple identical incidents - many variations possible
- ✦ Response needs to allow for varying incidents and conditions
- ✦ Reports produced need to be clear and specify all pertinent facts

9

Investigations

Since computer crimes are only increasing and will never really go away, it is important that all security professionals understand how computer investigations should be carried

out. This includes legal requirements for specific situations, understanding the “chain of custody” for evidence, what type of evidence is admissible in court, incident response procedures and escalation processes.

Incident Management

Many computer crimes go unreported because the victim, in many cases, is not aware of the incident or wants to just patch the hole the hacker came in through and keep the details quiet in order to escape embarrassment or the risk of hurting the company’s reputation. This makes it harder to know the real statistics of how many attacks happen each day, the degree of damage caused, and what types of attacks and methods are being used.

Although we commonly use the terms “event” and “incident” interchangeably, there are subtle differences between the two. An **event** is a negative occurrence that can be observed, verified, and documented, whereas an **incident** is a series of events that negatively affects the

company and/or impacts its security posture. This is why we call reacting to these issues “incident response” (or “incident handling”), because something is negatively affecting the company and causing a security breach.

Many types of incidents (virus, insider attack, terrorist attacks, and so on) exist, and sometimes it is just human error. Indeed, many incident response individuals have received a frantic call in the middle of the night because a system is acting “weird.” The reasons could be that a deployed patch broke something, someone misconfigured a device, or the administrator just learned a new scripting language and rolled out some code that caused mayhem and confusion.

Different Types of Assessments an Investigator Can Perform

- **Network analysis**

- Communication analysis
- Log analysis
- Path tracing

- **Media analysis**

- Disk imaging
- MAC (Modify, Access, Create) time analysis
- Content analysis
- Slack space analysis
- Steganography analysis

- **Software analysis**

- Reverse engineering
- Malicious code review
- Exploit review

- **Hardware/embedded device analysis**

- Dedicated appliance attack points
- Firmware and dedicated memory inspections
- Embedded operating systems, virtualized software, and hypervisor analysis



IR Planning

- ✦ Incident response team
 - ✦ Well trained, skilled, can make decisions
 - ✦ Coordinate with law enforcement/ external forensics experts
 - ✦ Clear roles and responsibilities
 - ✦ Clear procedures
- ✦ Organization level
 - ✦ System security: logging, integrity, monitoring, network IDS, etc.
 - ✦ User training
 - ✦ Data backup

10

When a company endures a computer crime, it should leave the environment and evidence unaltered and contact whomever has been delegated to investigate these types of situations.

All organizations should develop an **incident response team**, as mandated by the incident response policy, to respond to the large array of possible security incidents. The purpose of having an incident response team is to ensure that there is a group of people who are properly skilled, who follow a standard set of procedures, and who are singled out and called upon when this type of event takes place. The team should have proper reporting procedures established, be prompt in their reaction, work in coordination with law enforcement, and be an important element of the overall security program. The team should consist of representatives from various business units, such as the legal department, HR, executive management, the communications department, physical/corporate security, IS security, and information technology.

The incident response team should have the following basic items available:

- A list of outside agencies and resources to contact or report to.
- Roles and responsibilities outlined.
- A call tree to contact these roles and outside entities.

- A list of computer or forensics experts to contact.
- Steps on how to secure and preserve evidence.
- A list of items that should be included on a report for management and potentially the courts.
- A description of how the different systems should be treated in this type of situation. (For example, the systems should be removed from both the Internet and the network and powered down.)



IR Planning

- ✦ Interview relevant personnel
 - ✦ System administrators
 - ✦ Managers
 - ✦ End users
- ✦ Consider factors that determine the response
 - ✦ Has something similar been handled before?
 - ✦ Cost?
 - ✦ Origin of incident?
 - ✦ Legal issues?



IR Procedures

- ✦ Triage (detection): declare incident and initiate response
- ✦ Investigation: collect data
- ✦ Containment: isolate affected computers, change configuration, disconnect system, etc.
- ✦ Analysis: find out the root cause
- ✦ Tracking: the source (internal/external) and how
- ✦ Recovery: recover system and implement necessary fix

12

Incident Response Procedures

You should understand the following set of procedures (stages) for incident response:

- Triage: determine whether it is indeed an incident and whether the incident-handling process should be initiated.
- Investigation: involves the proper collection of relevant data, which will be used in the analysis and following stages.
- Containment: an infected server is taken off the network, firewall configurations are changed to stop an attacker, or the system that is under attack is disconnected from the Internet.
- Analysis: more data are gathered (audit logs, video captures, human accounts of activities, system activities) to try and figure out the root cause of the incident.
- Tracking: determine whether the source of the incident was internal or external and how the offender penetrated and gained access to the asset.
- Recovery: implement the necessary fix to ensure this type of incident cannot happen again. This may require blocking certain ports, deactivating vulnerable services or functionalities, switching over to another processing facility, or applying a patch.



Incident Response

- ★ Detection

- ★ Network traffic
- ★ System availability
- ★ Memory and CPU usage
- ★ Disk activity
- ★ Processes/applications/users
- ★ Abnormal activity
- ★ Modification (time, date, size)
- ★ System calls

=

13

When an event has been reported by employees or detected by automated security controls, the first stage carried out by the incident response team should be **triage**. Triage in this sense is very similar to triage conducted by medics when treating people who are injured. The crux of it is, “Is this person really hurt?” “How bad is this person hurt?” “What type of treatment does this person need (surgery, stitches, or just a swift kick in the butt)?”

So that’s what we do in the computer world too. We take in the information available, investigate its severity, and set priorities on how to deal with the incident. This begins with an initial screening of the reported event to determine whether it is indeed an incident and whether the incident-handling process should be initiated. A member of the incident response team should be responsible for reviewing an alert to determine if it is a false positive. If the event is a false positive, then it is logged and the incident response process for this particular event is complete. However, if the event is determined to be a real incident, it is identified and classified. Incidents should be categorized according to their level of potential risk, which is influenced by the type of

incident, the source (whether it’s internal or external), its rate of growth, and the ability to contain the damage. This, in turn, determines what notifications are required during the escalation process, and sets the scope and procedures for the investigation.



Incident Response

- ★ Incident investigation
 - ★ Compile information about the incident
 - ★ Collect data/evidence
 - ★ Host based data
 - ★ Live data
 - ★ Forensic duplication
 - ★ Network based data
 - ★ Logs
 - ★ Traces
 - ★ Process must ensure data integrity and adhere to policy, laws, and regulations

14

Investigation involves the proper collection of relevant data, which will be used in the analysis and following stages. The goals of these stages are to reduce the impact of the incident, identify the cause of the incident, resume operations as soon as possible, and apply what was learned to prevent the incident from recurring. It is at the analysis stage where computer forensics comes into

play. Management must decide if law enforcement should be brought in to carry out the investigation, if evidence should be collected for the purposes of prosecution, or if the hole should just be patched. Most companies do not have a forensics team on staff to carry out these tasks. In such situations, if a suspected crime has occurred and management does not want law enforcement involved but does want a forensics investigation carried out, external forensics experts need to be called in. An investigation must adhere to company policy as well as applicable laws and regulations.



Incident Response

- ✦ Incident Response Kit
 - ✦ Hardware
 - ✦ Requires higher end hardware
 - ✦ Should enable connectivity with varying systems
 - ✦ Disk space is critical especially for larger scale data collection
 - ✦ Mobility is key
 - ✦ Software
 - ✦ Different OS versions
 - ✦ Boot disks
 - ✦ Software that enables viewing of all types of files
 - ✦ Block level copy tools

15

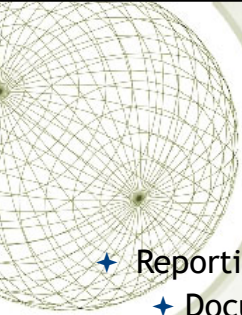
The next stage is **containment**. In the medical world, if you were found to have tuberculosis, you would be put in an isolation room because no one wants to catch your cooties. In the containment phase, the damage must be mitigated. In the computer world, this could mean that an infected server is taken off the network, firewall configurations are changed to stop an attacker, or the system that is under attack is disconnected from the Internet. A proper containment strategy buys the incident response team time for a proper investigation and determination of the incident's root cause. The containment strategy should be based on the category of the attack (that is, whether it was internal or external), the assets affected by the incident, and the criticality of those assets.

Once the incident has been contained, we need to figure out what just happened by putting the available pieces together. This is the stage of **analysis**, where more data are gathered (audit logs, video captures, human accounts of activities, system activities) to try and figure out the root cause of the incident. The goals are to figure out who did this, how they did it, when they did it, and why. Management must be continually kept abreast of these activities because they will be the ones making the big decisions on how this whole mess is to be handled.

Once we have as much information as we can get in the last stage and have answered as many questions as we can, we then move to the

tracking stage. (Tracking may also take place in parallel with the analysis and examination.) We determine whether the source of the incident was internal or external and how the offender penetrated and gained access to the asset. If the attacker was external, the team would contact their ISP to help them in gathering data and possibly help in finding the source of the attack. Many times this is difficult because attackers move from one system to the next, so several ISPs may have to get involved. Thus, it is important that the analysis and tracking team have a good working relationship with third parties such as ISPs, other response teams, and law enforcement.

Once the incident is understood, we move into the **recovery** stage, which means we implement the necessary fix to ensure this type of incident cannot happen again. This may require blocking certain ports, deactivating vulnerable services or functionalities, switching over to another processing facility, or applying a patch. This is properly called “following recovery procedures,” because just arbitrarily making a change to the environment may introduce more problems. The recovery procedures may state that a new image needs to be installed, backup data need to be restored, the system needs to be tested, and all configurations must be properly set.



Post-Incident Activity

- ✦ Reporting
 - ✦ Documentation needs to be done in a timely manner - delays should be avoided
 - ✦ Documentation should be clear and easy to understand by all parties involved in the investigation
 - ✦ Documentation should be standardized and templates should be derived to enhance and speed up the process of documentation
 - ✦ Communicate to press, customers, shareholders
- ✦ Review/Follow-up
 - ✦ Gather and discuss the lessons learnt
 - ✦ Use of data
 - ✦ Evidence retention

16

Closure of an incident is determined by the nature or category of the incident, the desired incident response outcome (for example, business resumption or system restoration), and the team's success in determining the incident's source and root cause. Once it is determined that the incident is closed, it is a good idea to have a team briefing that includes all groups affected by the incident to answer the following questions:

- What happened?
- What did we learn?
- How can we do it better next time?

The team should review the incident and how it was handled and carry out a post-mortem analysis. The information that comes out of this meeting should indicate what needs to go into the incident response process and documentation, with the goal of continual improvement. Instituting a formal process for the briefing will provide the team with the ability to start collecting data that can be used to track its performance metrics.