Unit 8 Availability and incident handling

Site:	Moodle - Edinburgh Napier University
Course:	INF11109 2019-0 TR1 001 - Security Audit & Compliance
Workbook:	Unit 8 Availability and incident handling
Printed by:	Timothy Muscat
Date:	Monday, 4 November 2019, 1:55 PM

Table of contents

Introduction

Incident recovery has been increasing in importance over the last few years and now needs to be seen as central to a risk management strategy. The diagram below situates availability within risk management as part of risk response.

In this unit, we cover the terminology and concepts associated with risk response: keeping information systems available after an incident or a disaster. The unit also explores how the concepts link together and the issues involved in their management.

Figure 8.1 Risk response

Figure 8.1 Risk management

Learning Outcomes

The learning objectives for this unit are:

1. Recognise the need for contingency planning and its relationship to risk management
2. Describe the main components of contingency planning
3. Understand the use of business impact analysis as a planning tool
4. Describe the main steps in recovery from an incident or disaster

Prescribed Reading

Prescribed reading for this section is noted below, and you will be prompted to read these as you progress through the unit:

- MIS Chapter 10 (Planning for contingencies)
- Baskerville, Spagnoletti, Kim (2014) Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management* 51(1) DOI: 10.1016/j.im.2013.11.004
- Bruce Schneier (2014) The future of incident response. Blog post: https://www.schneier.com/blog/archives/2014/11/the_future_of_i.html

8.1 Context: Why availability is becoming so important

Reading: MIS Ch 10 pp397-411 ("Introduction to contingency planning")

One way of looking at the increasing importance of incident response is explained by Bruce Schneier. He points out how 'Defectors' (the attackers) can take advantage of the gaps opened up by new technology before the defenders can react.

Figure 8.2 shows how the security gap gets bigger in times of rapid technological change, as it is more likely that at least one attacker will find a technical advantage. One implication is that responses have to be based around people and process, because by definition, any automated response could be compromised.

Figure 8.2 Availability Risk Curve

Figure 8.2 Availability Risk Curve
Source: Schneier B (2012) Liars & Outliers

8.1.1 Disasters and continuity: how the terms relate

Resilience is the other half of risk management: that is, it starts with impact analysis to prioritise the systems to defend (similar to what happens in risk management). The impact analysis is used as the starting point for incident response (IR) and disaster response planning (DRP).

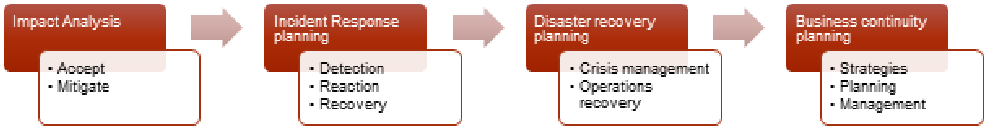

Figure 8.3 Resilience

Not illustrated in this diagram is the importance of post event review – where lessons are learned and processes improved.

The relationship between the terms is illustrated by the animation below.

Availability is an Information Systems concept.

- Information Security objective (familiar from the CIA triangle)
- Impact of lack of availability is different across systems and depends on criticality of systems: How long can users tolerate non-availability?

Continuity on the other hand is a Business concept.

- Covers all aspects of business, not just ICT
- However, most businesses are now dependent on ICT for availability of key information systems

'Disaster' bridges the gap between the two: a major ICT disaster can affect business continuity.

8.1.2 COBIT and ISO 27000 context

As would be expected, both COBIT and ISO27000 give prominence to availability.

ISO27000:2013 has two relevant domains: Information security incident management, and BCP : Information security aspects:

Figure 8.4 Information Security Aspects

Figure 8.4 Relevant ISO27000 domains

COBIT 5 core processes

COBIT 5 has three relevant processes:

- DSS04: Manage Continuity

– Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption

- DSS02: Manage Service Requests and Incidents

– Achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents

- DSS03: Manage Problems

In addition, there are aspects of incident handling in: DSS05.7: Monitor the infrastructure for security-related events and APO12.06 Respond to risk.

Figure 8.5 Processes

Figure 8 5 Continuity and incident handling being in the DSS domain in COBIT 5
Source: Any number of ISACA COBIT 5 documents

8.2 Incidents and responses

Reading: MIS Ch 10, pp412-424 ("Incident response")

8.2.1: Definitions

Incident

An **incident** can be defined as: the level of interruption in systems availability that appears to be temporary and is not expected to last longer than a few hours or days. It is containable without significantly impacting the business.

Incidents may be deliberately caused by an attack, or they may be a result of an accident or act of nature.

Incidents should be distinguished from **events**: NIST defines an event as "any observable occurrence in a network or system." This includes normal network operations, such as connections to servers, email transactions and database updates. Incidents are a type of event; not all events are incidents.

A **computer security incident** is:

> "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."

Remember: Non-security incidents can also bring your system down.

Reminder of core terms

As a reminder, four concepts underpin the discussion of incident handling:

Asset: Something that is worth protecting: Sensitive data, intellectual property, and access to critical operations are all assets. For example, user credit card numbers are an asset worth protecting in your application.

Threat: Potential occurrence, malicious or otherwise, that could harm an asset/ a bad thing that can happen to your assets. Threats cannot be managed (though they can be avoided).

Vulnerability: Weakness that makes a threat possible. This may be because of poor design, configuration mistakes, or inappropriate and insecure coding techniques. Weak input validation is an example of an application layer vulnerability, which can result in input attacks.

Vulnerabilities can be minimised, but they are inherent in connecting to the outside world: a vulnerability free system is also one that is shut off from the outside world: which is not really the point when running a business!

Attack: Action that exploits vulnerability or enacts a threat. Examples of attacks include sending malicious input to an application, or flooding a network in an attempt to deny service.

Elements of incident response planning

Incident response planning can broadly be said to have four elements.

1. Planning and preparation: Making sure all resources are in place to support detection and recovery.
2. Detection and assessment: Having processes in place which detect that an incident takes place (obviously, ideally, the incident would be prevented in the first place, but incident handling is essentially a detect and recovery control).
3. Responding: Containment, eradication and recovery - and collection of appropriate forensic data.
4. Learning lessons: What could have been done better? There will be a next time.

There are a number of IH frameworks which divide these four elements differently.

Figure 8.6 Incident management cycle

Figure 8.6 Incident management cycle

Remember - peparation makes everything possoble in the other elements of this cycle. If the policies, tools and training are not in place, it's very difficult to respond effectively.

8.2.2 Increasing importance of Incident Handling

In the relatively recent past, incidents were largely accidental or due to poor planning, as illustrated by this chart from 2008:

Figure 8.7 Incidents chart

Figure 8.7 Causes of application failures in 2008: mostly user error

However, the rise of targeted attacks such as advanced persistent threats (APT) and ransomware mean that the proportion of security breaches has increased significantly (though the other issues have not gone away). One way of looking at this is to understand the increasing sophistication and cost effectiveness of attacks, as illustrated below (from 2012) and the evolution has continued with the rise of ransomware and cryptojacking. The point is that attacks are likely to succeed, initially at least, hence the need for plans for identifying and responding to them.

Figure 8.8 Increasing sophistication and financial motivation behind attacks

Figure 8.8 Increasing sophistication and financial motivation behind attacks
(Source: ISACA (2014))

Schneier (2014) and (2017 in further reading) shows how thinking around incident handling is evolving. Technical support tools have also been evolving: security information and event management (SIEM) tools in particular, which combine security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts generated by network hardware and applications.

These articles illustrate the ongoing debate about how best to balance technology (analysis, automated responses) against the use of human insight and judgement during IR. Schneier makes a good argument that inherent uncertaintly combined with data overload does not help understanding what's going on - or what to do about it.

8.2.3 Incident management team

The incident response team needs to have a mix of technical staff… but also HR, Lawyers, and managers from affected departments. The team's membership may evolve over the period of a long-term incident.

Issues that teams face include:

- Being clear on the purpose
- When is the 'event' an incident? (Who can make this possibly very expensive decision?)
- Who is responsible for managing them?
- What is the process?
- Who can escalate, or declare incident over?

These teams are often known as the CSIRT (computer security incident response team).

Self-Assessment Question 8.1

The state of incident response

SAQ 8.1

Compare the Baskerville *et al* (2014) paper and the Schneier blog post and evaluate them as sources of useful knowledge. Then synthesise their content into a single statement on how incident response is evolving.

Questions

1. How would you justify using a blog post in academic work? Does it make a difference if you know who Bruce Schneier is?
2. How would you assess Baskerville, Spagnoletti and Kim as authors?
3. Having read the two papers, write a 1-2 sentence summary of how incident response is evolving according to both papers. Are there any interesting additional information that each adds?

Self-Assessment Question 8.2

Now try the following.

Use these notes and what you have found from your reading to construct a model of incident handling.

- How many steps are involved.
- Where does the process start? ...and end?

Reflective Exercise 8.1

Read these articles and critically review them against general principles of incident handling- relate them to a workplace with which you are familiar if you can:

- ARS Technica (2015) “EPIC” fail—how OPM hackers tapped the mother lode of espionage data
- Troy Hunt (2016) The emergence of historical mega breaches
- Dark Reading (2016) Ransomware Doesn’t Have To Mean Game Over

1. ARS Technica (2015) “EPIC” fail—how OPM hackers tapped the mother lode of espionage data

2. Troy Hunt (2016) The emergence of historical mega breaches

3. Dark Reading (2016) Ransomware Doesn’t Have To Mean Game Over

8.3 Disaster recovery and BCP

8.3.1 Main concepts

Reading: MIS Ch 10: pp431-450 ("Disaster recovery", "Business continuity", "Crisis management", "Business resumption")

Disaster recovery planning (DRP) exists on the same spectrum as incident responses.

Figure 8.9 Disater Recovery Planning

Figure 8.9 Disaster Recovery Planning

A disaster is defined as an event that causes significant and perhaps prolonged disruption in system availability.

That is, there is a significant impact on the (whole) business, not just the ICT infrastructure. Disasters can be man-made (intentional or not) or natural.

DRP must allow for flexibility, and clarity on responsibilities and priorities are most important. There is a close relationship between Impact analysis and Recovery planning.

8.3.2 Business impact analysis as a planning tool 3

DRP has four key stages:

- Define business process: Documenting criticality, role. This should tie into risk assessment process. Perspective is different: here it is "what would we do if this broke" – ie impact not likelihood
- Identify infrastructure that supports the process
- Determine tolerances: How easy would it be to go on?
- Plan for harm reduction: Reducing likelihood of interruption and impact of interruption

Critical systems are judged by their importance to the business (including key stakeholders affected). They can also be judged by tolerance (how many days can the system be down before the business is impacted), cycles (are there particular times when the system is most critical to the business – e.g. payroll systems) and data recovery (how easy is it to recover data if the system does go down).

8.3.3 Recovery strategies

As with incident handling, the DRP team will include members with a range of roles, including:

- Champion
- Project manager
- Team members
- Core functions: IT, HR, legal
- business managers

The team will be organised by phase & incident type: Skills and priorities for immediate response are different from implementing recovery as illustrated below:

Figure 8.9 Example phases in disaster recovery

Figure 8.9 Example phases in disaster recovery

Three acronyms summarise the core concepts of DPR as illustrated in Figure 8.9 below:

- Recovery Point Objective (RPO): Last available data backup, which defines the state the system will be in after restoration.
- Maximum tolerable outage (MTO): The period which the system can be down before the business itself is threatened.
- Recovery time objective (RTO): How much time is available between a disaster being declared, and the MTO being reached.

8.3.4 Recovery strategy: sites

DRP has to take into account the possibility that the original site may not be available. Classic models for handling the loss of the normal operational site include: Hot sites (live replication of systems), Cold sites (infrastructure only). Warm sites (where basic hardware is in place but systems and data need to be uploaded before operations can be resumed). Sites could be fixed buildings, or mobile (trailers etc).

Disaster Recovery as a Service (DRaaS)

There are a number of alternatives to the traditional site-based approach. The most significant nowadays is cloud based services (simply bring up a new server) and/ or virtualisation, as explained by these sales videos:

Of course, DRaaS adds new critical points of failure of its own... for instance:

- Is there network capacity available which can support connection to the recovery infrastructure?
- What happens if several DRaaS clients are affected at once?

Reflective Exercise 8.2

Please attempt the following:

RE 8.2

Look for information on DRP where you work (or Edinburgh Napier's website).

- Is there a published plan?
- How would you assess it against what you have learned here? (you can answer this part even if you could not find an actual plan)

8.4 Testing strategies

Reading: MIS Ch 10: pp453-454 ("Testing contingency plans")

The aim of testing is to improve the plan's effectiveness and identify vulnerabilities, faults, inefficiencies. It is often argued that the main benefit of testing is in fact getting people within the organisation to practice working together.

Testing strategies can be listed as follows, in increasing order of effort and risk:

1. Desk check

2. Structured walkthrough

3. Simulation

4. Parallel testing

5. Full interruption

They are described in detail in the prescribed reading.

8.5 Case Study: TravelFar

Read the TravelFar background brief below then answer the questions which follow.

Background Information

You work in the incident response and business continuity unity for TravelFar Hotels, a US company with headquarters in Charlotte, North Carolina, USA. There are six regional offices scattered throughout the various geographical subregions within the eastern part of the US.

You report to the chief information security officer (CISO). TravelFar also has a contract with a large consultancy that enables you to obtain technical consultants from this company in two hours or less if an urgent security breach and/or business continuity incident occurs.

The company markets itself as a midtier hotel chain, one in which travellers pay a fair price to obtain a clean, safe and suitably sized, but not elaborate, room and that offers no additional cost 'extras' such as free breakfast, Internet access or movies. Additionally, although TravelFar is by no means new, it has expanded substantially over the last few years by buying land near locations where automobile traffic flow tends to be heavy in a number of cities. TravelFar paid a premium for this land; however, the dividends have been rich, the new hotels now generating the greatest amount of per hotel revenue. TravelFar has incurred significant debt (albeit most of it at a relatively low interest rate) to purchase land and to build new hotels and finance is now more difficult to obtain.

The hotel industry is extremely competitive, with an abundance of economy, midtier and luxury hotels scattered throughout the world. The major advantage that TravelFar Hotels holds is that its programming team, in connection with certain TravelFar employees and external consultants, has developed a decision-aiding application that provides detailed information concerning the potential viability of land for sale at the potential site of a new hotel. In the last five years, TravelFar has used this application to evaluate many hundreds of potential sites; every land purchased during this time period has resulted in a more profitable than average hotel being built.

Each regional manager is expected to make as much profit as possible and brutal competition amongst regional managers to 'make the best numbers' exists. The two top regional managers are rewarded handsomely with generous perks and big salary increases and bonuses, and the only way to move higher in the organisational chart is to be one of the top two regional managers during any year. Promotion at higher levels of management is always from within.

Most regional managers now also realise that the key to optimising their region's profits is expanding the number of hotels in their region, but to do so, they have to dip into their region's operating funds because TravelFar corporate pays for most, but not all, of the cost of building each new hotel.

The issue

Safeguarding this land site evaluation application and its output is one of the highest priorities of the information security function. Additionally, the company's procurement and payment systems are extremely critical to its business operations.

Recently, a rumour circulated around the company that someone from one of the regions tried to tamper with the land site evaluation application in a manner that would result in inaccurate output for all regions except for the one in which this person works. The application and the machines on which it runs appeared not to have been tampered with, but now an even greater issue has surfaced—could an outsider penetrate TravelFar Hotel's exterior network defences to reach and then tamper with this application and its data and the company's procurement and payment systems?

Also, this company's public-facing web servers that enable customers to make and modify hotel reservations are within TravelFar's corporate network, which could potentially allow anyone who was able to break into one of these servers to launch attacks directly at the land site application, the payment system and the procurement system without any major intervening network security device such as an internal firewall.

Your role

You must help develop an incident containment plan as a part of a larger incident response plan for TravelFar Hotels. This plan will apply to the land site evaluation application, the procurement system and the payment system, all of which senior management deems equally critical from a business perspective. All three applications are distributed, three-tier web applications in which clients connect to a server that has a back-end database.

In the opinion of many experts, containment is the major difference between successfully and unsuccessfully handling an incident. If containment plans are inadequate (e.g., because they do not specify all the steps needed) or if they are not properly followed, a security incident that initially appears to be small may proliferate out of control, costing an organisation millions of dollars from a disruption in operations and labour costs associated with response operations. In comparison, containment done properly can reduce the duration and impact of an incident to a minimum. (Remember, the main goal of incident response is to reduce incident-related risk to an acceptable level.) Your inclusion of all necessary containment steps for each type of incident listed previously is, thus, imperative.

Case study questions

Now answer the following.

1. Why does the company need an incident response plan? (Imagine a senior manager has asked you this - so explain it in a simple way that makes business sense)

2. Which of the confidentiality, integrity, and availability (CIA) triad is most critical to this company's business goals, and why?

3. Incident Planning

A commonly used incident response model includes the following stages—preparation, identification, containment, eradication, recovery and follow-up. During the containment phase, the fact that an incident has occurred will, thus, already have been confirmed.

Choose one of the incident types from the list below and draft the bullet points for your plan.

1. Malicious code

2. Insider tampering with code

3. Outsider tampering with code

4. Insider tampering with data

5. Outsider tampering with data

6. Malicious destruction of an application and/ or database

You need to include the kinds of steps that are involved in the containment stage and state specifically how these will be applied in each of the following steps:

Step 1a: Preparation:Policy

Step 1b: ICT systems

Step 2: Identification

Step 3: Containment

Step 4: Eradication

Step 5: Recovery

Step 6: Follow-up

Further Reading

- VMWare (2010) The Top Ten Most Forgotten Things When Building a Disaster Recovery Plan
- Schneier (2017) Security Orchestration and Incident Response - https://www.schneier.com/blog/archives/2017/03/security_orches.html

End of Unit Summary

This unit was structured to build your understanding and awareness of risk management. Learning activities were geared to help you critically reflect upon the practical and theoretical issues associated with establishing risks, responding to them, and to link this to your own work experiences and practice.

In summary, there are two aspects to planning for incidents and disasters:

- Knowing what do to, in terms of incident reporting, but also clear policies, reporting lines, authorities, etc.
- Testing it. For critical infrastructure, this could include participation in & integration with industry-wide, national or EU-wide exercises

In both cases, it can be important to consider the supply chain - key suppliers and customers could need to be involvedin in diferent stages of the planning.

This Top 10 forgotten things from VMWare whitepaper from 2010 is still relevant:

1. Failure to identify all key threats
2. Creating a plan with too few people
3. Lack of auto-notification processes
4. Failure to procure adequate backup power
5. Forgetting to prioritise resources for restoration
6. Inadequate documentation & communication of plans
7. Relying on (untested, old) backups
8. Not testing the plan
9. Passwords too hard to find (or override)
10. Not keeping the plan up to date

Before getting too fancy, it’s worth making sure that these basics are covered.

When you are ready, try the End of Unit Progress Test for Unit 8

Before you leave this unit

If you have completed this workbook, please click on the **Submit All Answers and Finalise Workbook** button below.

You can now move on to Unit 9 Audit & Controls.