Business Continuity Planning

Tom Olzak, MBA, CISSP

February 2018

Business continuity planning (or contingency planning) is an important part of security. It directly supports the availability portion of the security triad: confidentiality, integrity, and availability. Business continuity planning (BCP) involves looking forward, ensuring operation of business processes during attacks, system component failures, or catastrophic events.

The content of this document is based on the CISSP Common Body of Knowledge. More detailed discussions for some topics covered are available via the links at the end of this lecture.

What is BCP?

BCP includes planning for disasters, but disasters happen much less frequently than smaller events. Server or switch failures are much more likely than a tornado taking down a data center. BCP includes looking at things that might (and will) interrupt business processes, especially single points of failure. Disaster recovery plans are implemented with business continuity activities fail. Stewart, Chapple, and Gibson (2015) write

> "One easy way to remember the difference is that BCP comes first, and if the BCP efforts fail, DRP steps in to fill the gap. For example, consider the case of a datacenter located downstream from a dam. BCP efforts might involve verifying that municipal authorities perform appropriate preventive maintenance on the dam and reinforcing the datacenter to protect it from floodwaters" (Kindle Locations 3500-3502).

BCP is another form of risk analysis. It looks at the cost to the business if business processes are not available for some reason. A formula for this is

P x M = C

- **P**robability of harm. What is the probability that a planned for event might occur? What threats to continuity exist, what are the continuity vulnerabilities, and what is the likelihood that an event (threat leveraging a vulnerability) will occur. This is annualized.
- **M**agnitude of harm. What is the business impact if the event occurs? This is also annualized.
- **C**ost. What is the potential annual cost to the business for the event under study?

This is another way of looking at the risk formula RISK = THREATS x VULNERABILITIES x BUSINESS IMPACT. And in both models, we annualize the numbers.

Annualizing Impact

We annualize because whatever we do to mitigate costs involves the annual budget. We need to sell mitigation to management based on annual loss vs. annual prevention cost. If the cost in this year's budget is $50,000 annually to prevent $40,000 in potential annual losses, management will likely accept the business interruption cost. However, if we can come up with a solution that is annually $20,000 for the same event, it is very likely you will get approval for the budget dollars.

Annualizing cost begins with determining a probability factor. For example, assume that a specific event will occur, on average, every three years. We annualize this by dividing 1 (100% probability) by 3, arriving at .33 (annual 33% probability). Consequently, when we multiply .33 by the magnitude of harm, we arrive at an annual cost.

Using real numbers, we determine that a server failure will likely take down a specific critical process every 5 years (based on mean time before failure). This results in an annualized probability of occurrence of 1 / 5 = .20.

If this system fails, it will cost the company $100,000 per day. Based on existing response capabilities, it will take about 2 days to recover the process. Therefore, the total cost of an event is $200,000. We multiply this by the annualized probability of occurrence (.20 x 200,000), resulting in an annual cost for this event of $66,000.

The BCP Process

BCP is continuous and should be part of every project plan and all change management risk reviews, it begins with policy. Management must initiate BCP activities by establishing expectations about ensuring business process availability. An example of a BCP policy is available from SANS.org. This policy is titled Disaster Recovery, but it is easily extended to all BCP activities.

Once the policy is in place, the organization needs a documented process for determining business interruption risk. Stewart, Chapple, and Gibson write that the steps to ensuring good BCP are

1. Project scope and planning
2. Business impact assessment
3. Continuity planning
4. Approval and implementation (Kindle Locations 3511-3512)

These steps form a complete project when initially performed… when no business continuity or disaster recovery plan exists. Once plans do exist, they are steps contained within every IT project and ensured with a strong change management process.

Project Scope and Planning

When a business continuity plan does not already exist, project scope includes identifying all critical business processes. This should have already been done when the organization performed an overall risk assessment. Every organization should start its security management activities by identifying critical systems. If this has not been done, the organization is likely throwing money at security without focusing on what addresses the most risk.

Updating the list of critical processes and associated infrastructure is part of any change management process. Making necessary changes to all system documentation, including recovery processes, must be included in any update or replacement project.

When creating an initial plan or managing an existing plan, we need a team that makes recovery decisions. According to Stewart, Chapple, and Gibson, we do this by identifying

1. Operational departments that are responsible for the core services the business provides to its clients
2. Critical support services, such as the information technology (IT) department, plant maintenance department, and other groups responsible for the upkeep of systems that support the operational departments
3. Senior executives and other key individuals essential for the ongoing viability of the organization (Kindle Locations 3529-3532)

The BCP team should represent all identified stakeholders. These three steps also help us ensure we address all critical processes.

Business Impact Assessment

For each business process, the BCP team determines the business impact if the process unexpectedly stops. One of the first steps in this process is calculating the process maximum tolerable downtime (MTD); how long can the process be down before the business suffers irreparable harm? Critical process recovery should come before this time expires.

In addition to MTD, the team should also work with the business to determine the business impact of process downtime. Business impact always happens, even if the MTD is not reached. As with risk assessments, this impact can be either quantitative or qualitative.

Quantitative impact is represented by actual dollar amounts. Qualitative impact is represented by values. A hybrid approach uses both dollars and values when complete dollar analysis is not possible.

One important consideration during impact analysis is how regulations might affect process downtime.

Continuity Planning

During impact analysis, the team prioritizes processes and associated infrastructure. During continuity planning, the team determines how to manage the business impact identified. As with any risk, the team can recommend to

- Accept
- Reduce (mitigate)
- Assign (transfer)
- Reject (not recommended)

Accept or reduce

Business impact is usually accepted if the annualized cost of mitigation is more than the projected annualized cost of a process failure. The cost of mitigation involves multiple elements:

- Implementation costs: Is additional infrastructure required to remove single points of failure? Is it necessary to engage a third-party hot site, cold site, or hybrid warm site provider? Is creation of a co-location a better choice? What would be the cost of simply moving systems to a cloud service provider?
- Training: Will staff need new skills to use implemented mitigation solutions? What is the cost of training? Is it necessary to hire someone who already has experience?
- Annual maintenance: If additional software or hardware is implemented in the data center, what are the annual maintenance fees?
- FTE costs: One FTE (full time equivalent) is the salary, tax, and benefit costs of one employee qualified to maintain/manage the implemented solutions. What is the cost of the needed FTE? How many FTEs are needed? What is the annual cost of these FTEs? Is additional staffing needed? Are these FTEs taken from other tasks? If so, what are the opportunity costs?

When determining how to reduce impact, be sure to consider availability of rebuild documentation, easily accessible configuration files, recovery time objectives, and maximum time to repair.

Assign

Assigning is the transfer of the cost associated with an event. This is usually done by purchasing cyber insurance. When assessing insurance, be sure your attorneys read the fine print about what is actually covered… or not covered. In some cases, the organization might be able to contractually obligate a vendor or cloud service provider to assume some or all of the cost. What management can never transfer, however, is ultimate responsibility for ensuring the continued operation of the

organization. The other costs not transferrable are associated with loss of customer and investor confidence: short term and long term.

Approval and Implementation

The approval and implementation process is not a project. It is a process. It continues after the initial BCP project ends. What follows is the documentation and implementation of an initial BCP. Following this, we will look at how we integrate a BCP process into all process and infrastructure changes.

Approval

If management supports the BCP policy and is fully engaged and trained in BCP (usually trained by the BCP team), approval of an overall plan or a plan for specific system is not difficult. But any approval requires the team to present its findings and recommendations in a way management cares about.

When making any risk management presentation to management, it is always about the impact to the bottom line. In many organizations, ethical conduct by the business is also a big consideration (it should always be, but…). Consequently, when the team creates its presentation, it is important to explain how the continuity vulnerabilities (prevention, detection, and response) can significantly reduce profits or cause significant harm to customers, employees, investors, and other stakeholders.

Implementation

Initial implementation of a BCP involves three primary activities: documentation; training and education; and maintenance. Ensuring maintenance is part of documentation, but we look at it separately, here.

Documentation

According to Stewart, Chapple, and Gibson, document should accomplish the following:

- "It ensures that BCP personnel have a written continuity document to reference in the event of an emergency, even if senior BCP team members are not present to guide the effort.
- It provides a historical record of the BCP process that will be useful to future personnel seeking to both understand the reasoning behind various procedures and implement necessary changes in the plan.
- It forces the team members to commit their thoughts to paper— a process that often facilitates the identification of flaws in the plan. Having the plan on paper also allows draft documents to be distributed to individuals not on the BCP team for a "sanity check'" (Kindle Locations 3910-3915)

The document should contain the following sections

- **Continuity Planning Goals**. This section defines the BCP goals focused on by the team during plan design. It should also include a statement of management support.

- **Statement of Importance**. The document must clearly explain why business continuity activities are important to the business, its employees, its customers, and its investors. It explains that the continued viability of the organization depends on the plan.

- **Statement of Priorities**. During critical process identification and business impact analysis, the team prioritized processes and related business continuity activities. This section should list all critical business processes listed by importance to the organization.

- **Statement of Urgency and Timing**. During an initial BCP planning project, an action is completed to bring the organization's risk to an acceptable level. The action plan includes prioritized tasks to mitigate risk associated with likely process failures and associated business impact. It assigns a responsible resolution team or person and a remediation completion date.

- **Risk Assessment**. This is the documented analysis of the probabilities of harm and the associated business impacts identified for each critical business process.

- **Risk Mitigation/Acceptance**. This section is very important. It explains why each risk is mitigated, accepted, or transferred. For presentation to management, these are the team's recommendations. For the final document, this is modified to reflect management's decisions and the reasons for those decisions. This is important information for future audits and justification when the inevitable business continuity event happens.

In addition to the initial report and plan, the team should ensure an incident response plan exists. The organization should consider integrating business continuity response in attack response processes. In this way, the same team is trained and ready to respond to any interruption to business processes. Stewart, Chapple, and Gibson write that the response plan should include

- "Immediate response procedures (security and safety procedures, fire suppression procedures, notification of appropriate emergency-response agencies, etc.)

- A list of the individuals who should be notified of the incident (executives, BCP team members, etc.)

- Secondary response procedures that first responders should take while waiting for the BCP team to assemble" (Kindle Locations 3991-3994)

Training and education

No security activity is successful unless those responsible are regularly trained and tested. BCP training and education begins with all system design and management teams being aware of how to identify and manage continuity vulnerabilities. In every project, in every modification activity, new or modified system designs must be reviewed for these vulnerabilities.

Business continuity awareness must extend throughout the SDLC. All IT personnel must understand what business continuity vulnerabilities look and what to do when identified. This helps locate and manage any vulnerabilities missed during project, change management, and risk reviews.

Maintenance

Ensuring continuous attention to business continuity is part of the risk review in the change management process. The purpose of change management is to ensure the implementation of new systems or modification of existing systems without breaking anything: including information security risk, failure of business process operation after the change, or the introduction of business continuity risk. Consequently, all reviewers involved in change approval, including members of the change advisory board, must be aware of what constitutes a business continuity vulnerability.

Another activity in which an organization can identify business continuity vulnerabilities is the risk assessment. Each critical system and related networks should be assessed at least once per year. Including business continuity in risk assessments is necessary if an organization wants to identify and manage all business risk.

Takeaways

- Business continuity planning is necessary to ensure complete coverage of the CIA triad "availability" element.
- BCP includes disaster recovery. However, disasters are a small part of overall continuity planning. BCP must include any vulnerability, no matter how small, that might interrupt one or more critical business processes.
- Implementation of business continuity management begins with a policy and continues with integrating business continuity tasks in all design, implementation, and change management processes.
- Business continuity management should permeate all IT activities
    - Design and implementation
    - Risk assessments
    - Change management
    - Daily activities

Additional BCP Information
For more information on this topic, see

- The elements of business continuity planning
- Business Impact Analysis
- FEMA Business Impact Analysis Worksheet
- Six Steps to Implementing ITIL Change Management
- Incident Management and Response Guide
- It's all about critical business processes
- Business Continuity Event Planning: Framework for root cause and continuous improvement analysis

References

Stewart, J. M., Chapple, M., Gibson, D. (2015). CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide. Wiley. Kindle Edition.