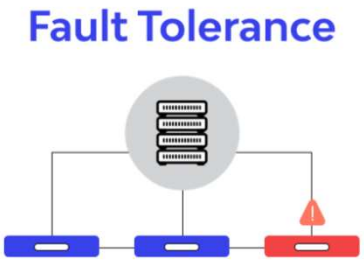
IT Fundamentals

CHAPTER 11:

BUSINESS CONTINUITY AND COMPUTER SUPPORT

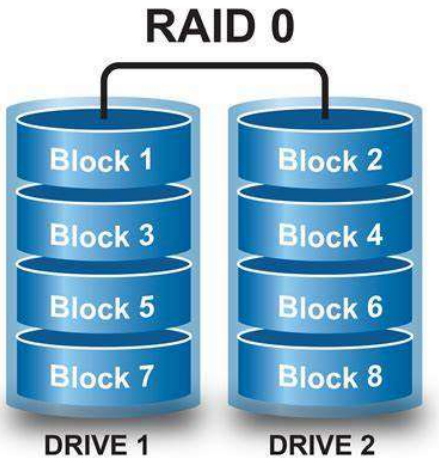
Fault Tolerance

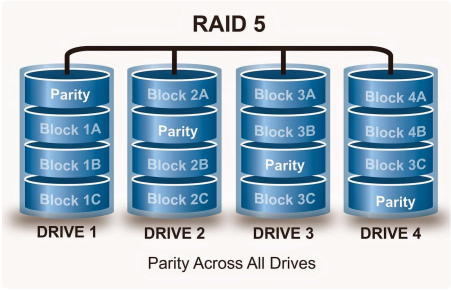


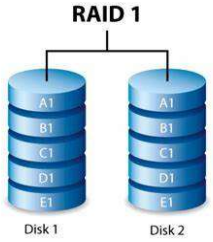
- Contingency plans
  1. Perform business impact analysis
  2. Identify preventive systems
  3. Develop a recovery plan
  4. Test the recovery plan
  5. Set up a maintenance and review schedule
  6. Implement training

Replication and Redundancy

- Data redundancy
  - RAID 0
  - RAID 1
  - RAID 5
- Network redundancy
- Power redundancy







Importance of Computer Backups

- Importance of data
- How easily replaceable is it?

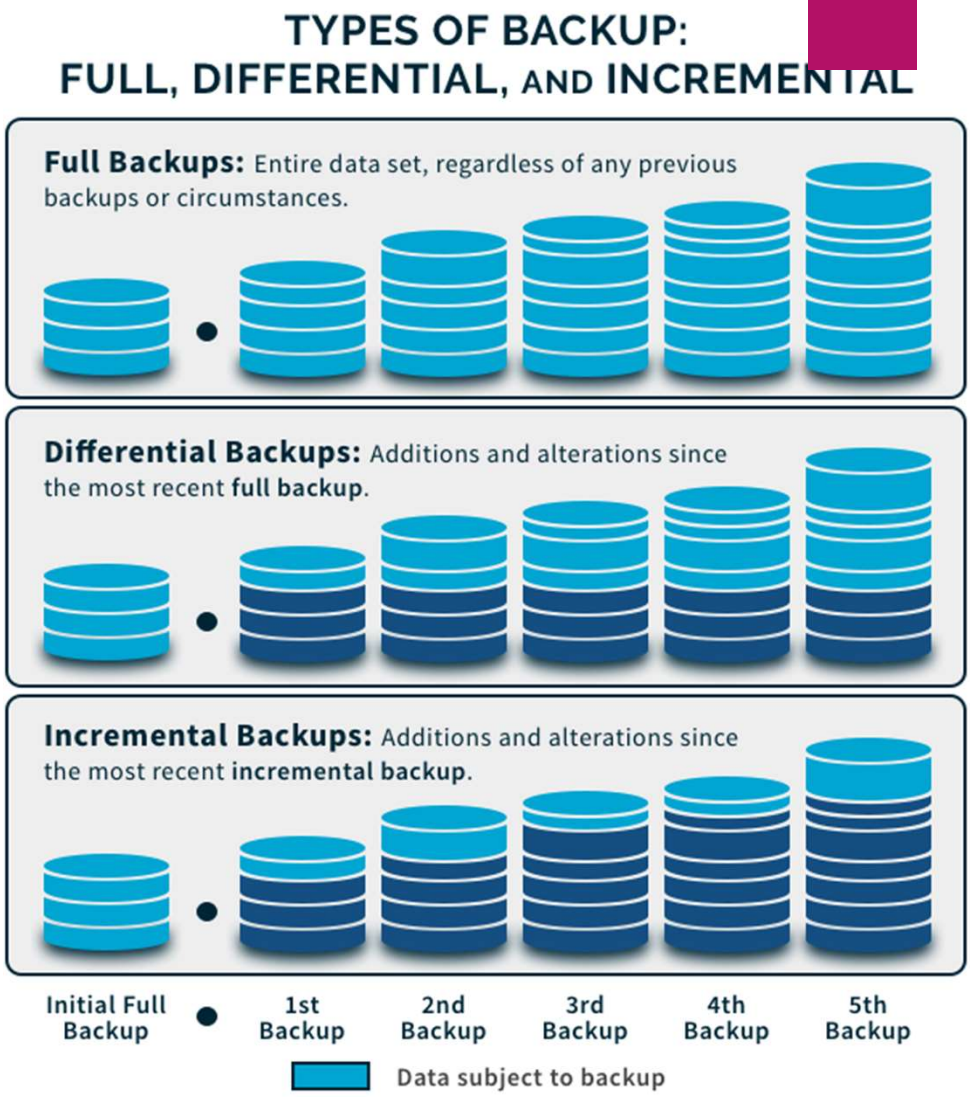
How Backups Work

Archive bit

Backup software programs

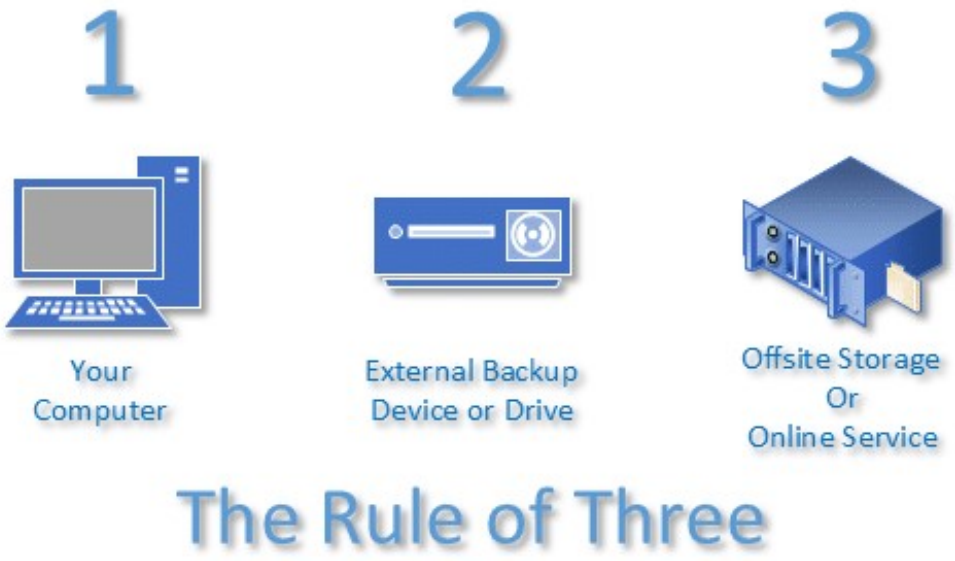
Backup Types

- Normal
- Copy
- Incremental
- Differential
- Daily



Backup Locations

- Locally attached storage
- Network attached storage
- Internet or cloud-based



Backup Frequency and Scheduling

Frequency depends on rate of change and importance

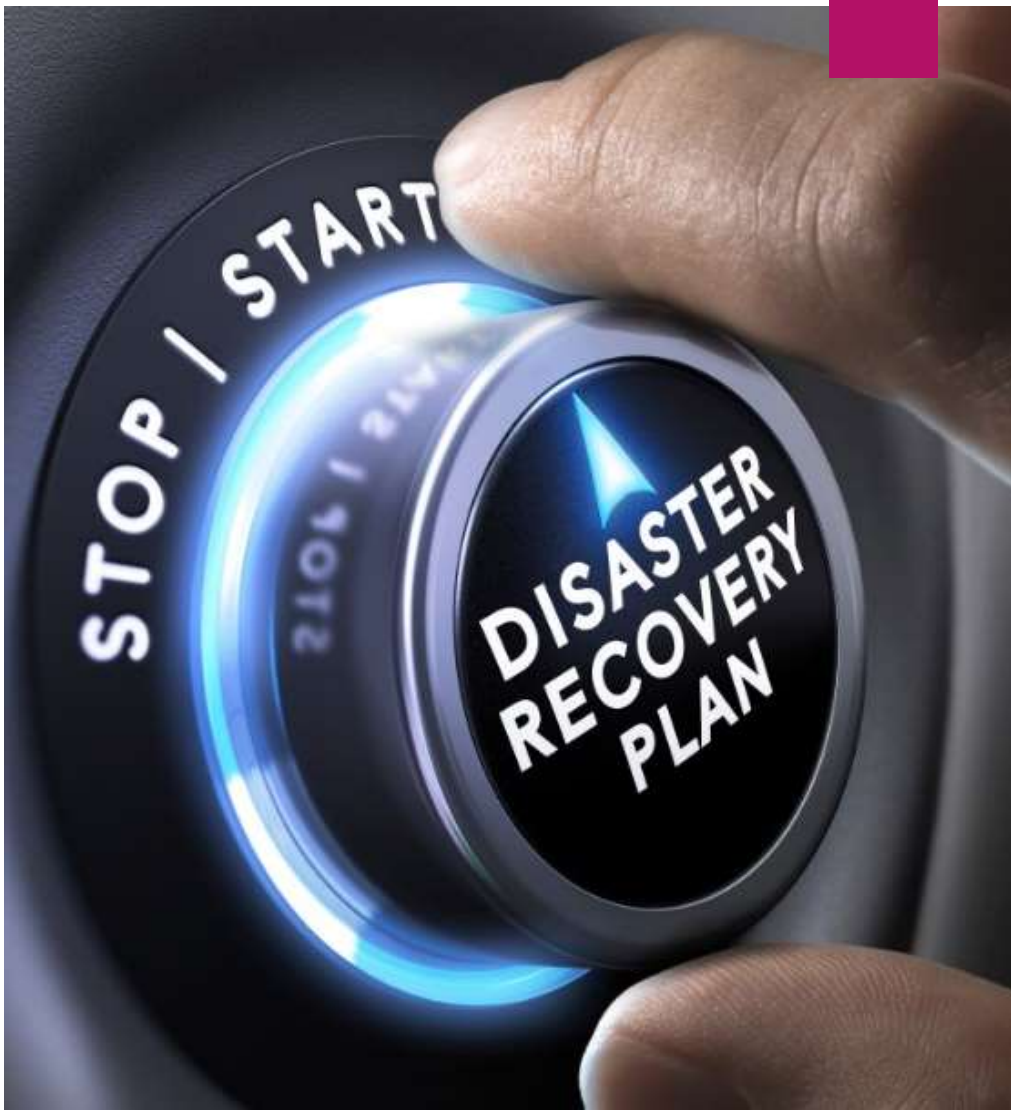
Scheduling prevents forgetting

Backup Verification and Testing

- Important step
- Frequently overlooked
- Won't know something is wrong until it's too late

Disaster Recovery

- Have a plan in place
- Train appropriate personnel on plan
- Clearly documented



Troubleshooting Theory

- Identify the problem
- Research knowledge sources, if applicable
- Establish a theory of what's wrong
- Test the theory
- Establish a plan of action to fix the problem
- Implement the solution
- Verify functionality
- Document the findings

Identifying the Problem

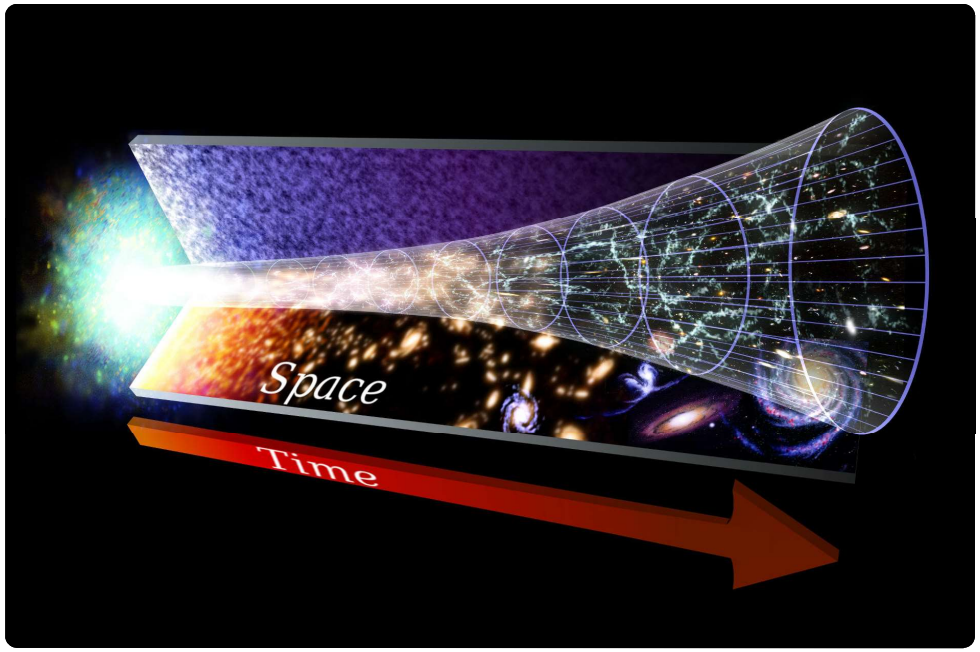
- Talk to the user/customer
- Gather information
- Try to isolate the issue
  - When/where/how does it happen

Research Knowledge Sources

- Manuals
- Manufacturer web sites
- Google
- Forums/blogs

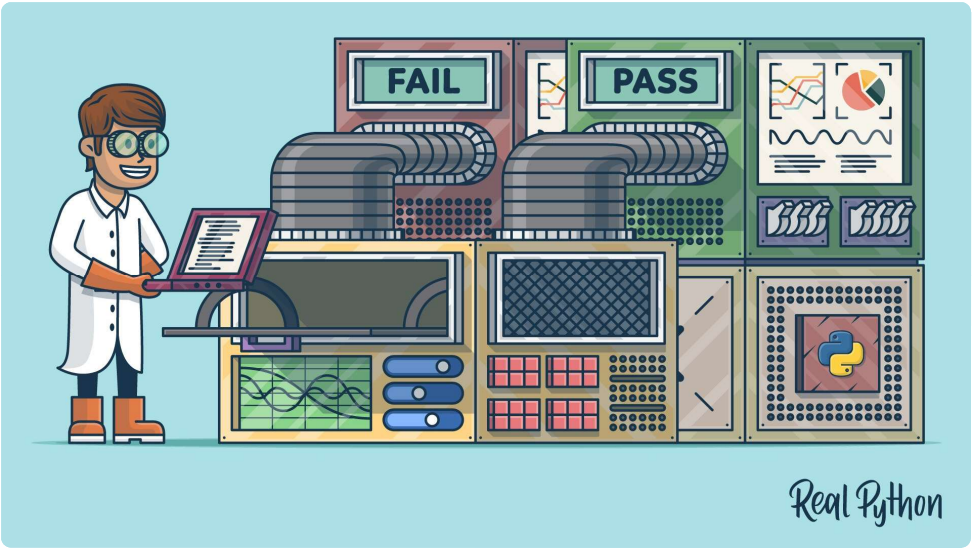
Establish a Theory

- Question the obvious
- Eliminate possibilities
- Divide and conquer



Testing the Theory

- Check the simple stuff first
- Check to see if it's user error
- Restart the computer

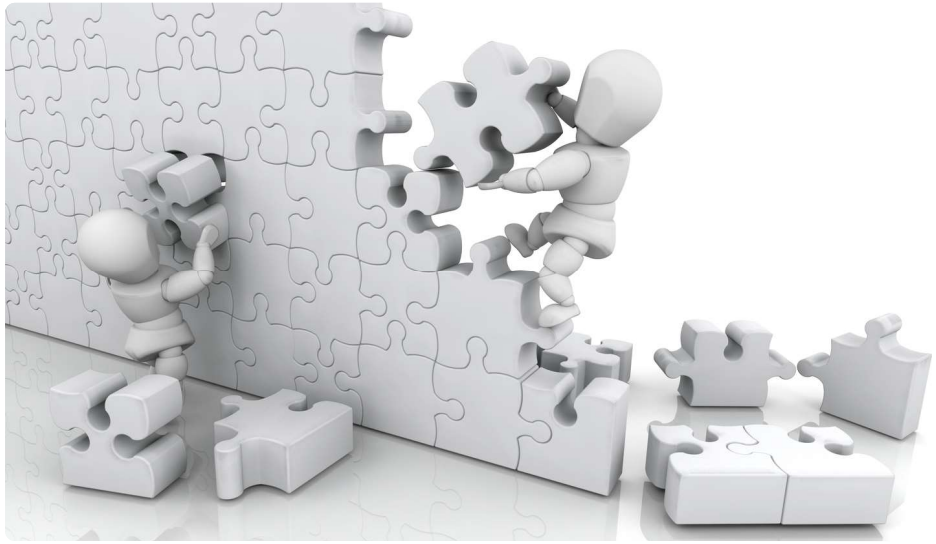


Establishing a Plan of Action

- The fix might or might not have worked
- If needed, try again
- Spread the solution as needed
- Document the solution (take notes)

Implement the Solution

- If the problem was isolated, you may not need this step
- Reapply fix to other computers as needed
- Escalate if necessary

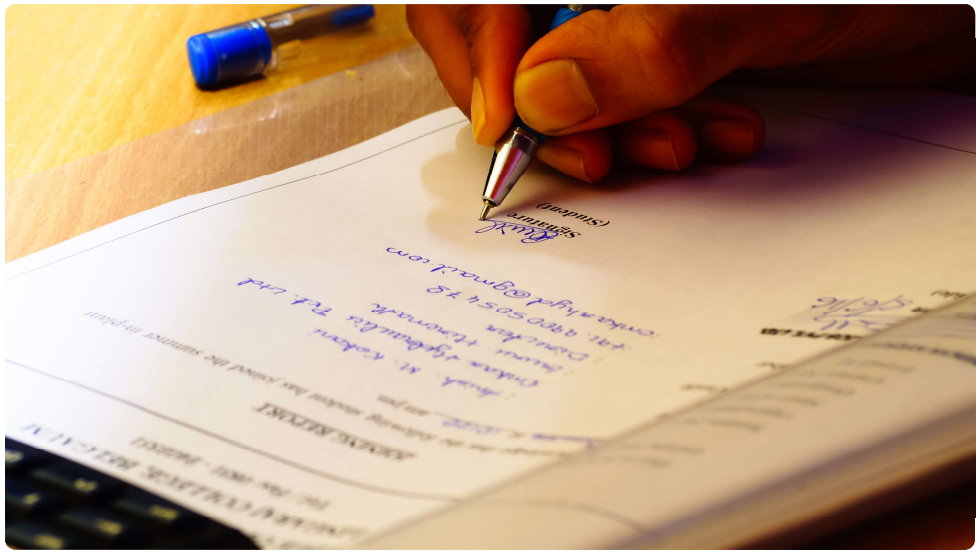


Verifying Functionality

- Be sure the error or problem is not coming back
- Check other major systems or applications to ensure the fix didn't cause obvious problems

Document the Work

- Most critical step!
- Carry a notebook
- Design a process that works for you
- Use openly available journals if multiple people troubleshoot problems

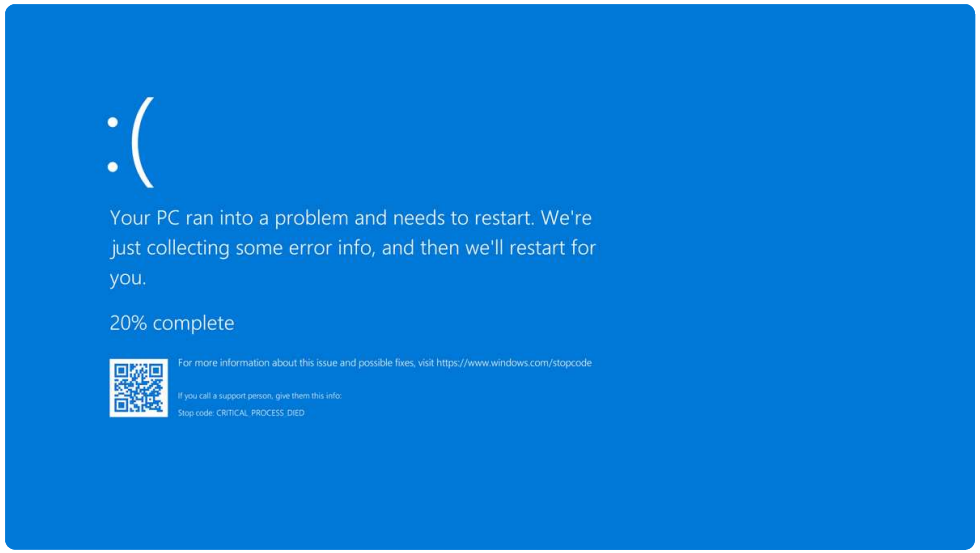


Troubleshooting Examples

- Computer won't boot up
- Operating system errors
- Application failures
- Hardware failures

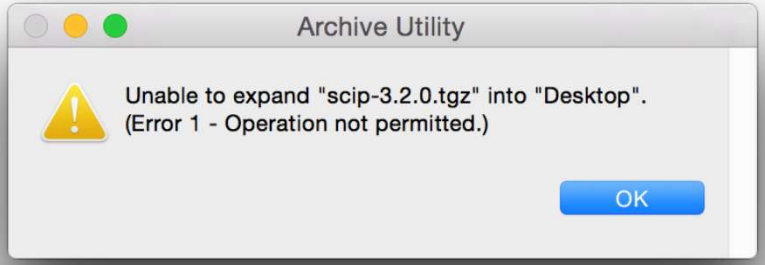
Computer Won't Boot

- Nothing on the monitor
- Black screen or blue screen
- Windows won't load
  - Using Safe Mode
  - Using System Restore
  - Using the System Configuration utility
  - Using the Recovery Environment
- Mac OS X won't load



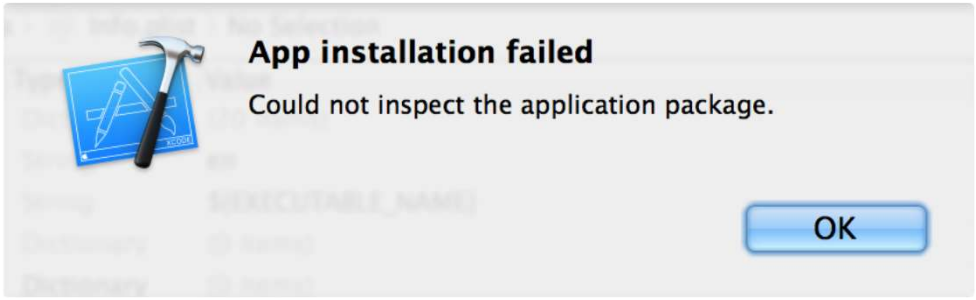
Operating System Errors

- Look for error messages online
- OS slowdown or lockup could be overheating



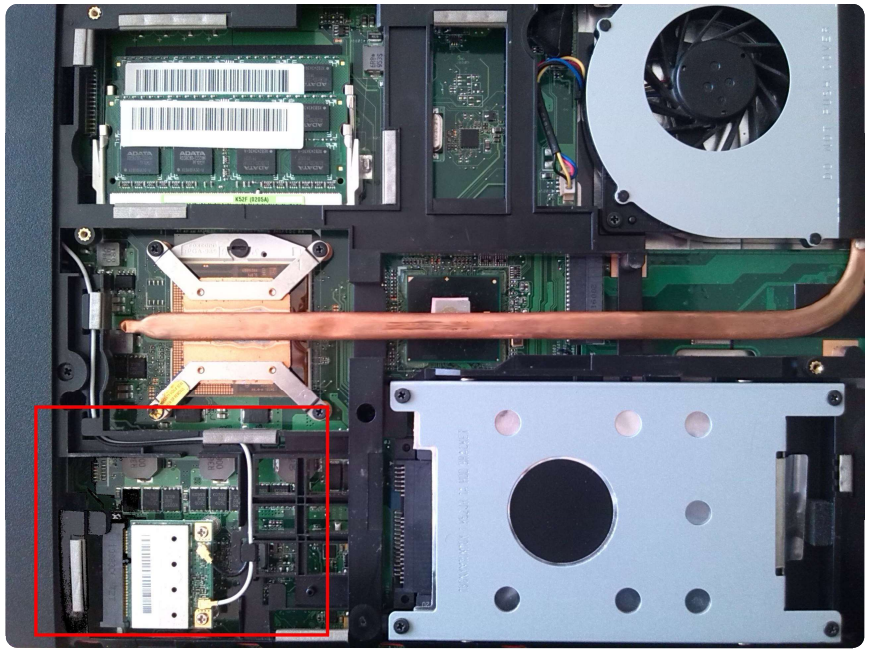
Application Failures

- Application fails to install or fails to run
- App used to work, but no longer does
- Persistent application crashes



Hardware Failures

- Hardware/driver compatibility issues
- Malfunctioning input devices
- Troubleshooting network connectivity



Chapter 11: Business Continuity and Computer Support

- Explain the troubleshooting methodology
  - Identify the problem
  - Research knowledge base/Internet, if applicable
  - Establish a theory of probable cause
  - Test the theory to determine the cause
  - Establish a plan of action to resolve the problem and identify potential effects
  - Implement the solution or escalate as necessary
  - Verify full system functionality and, if applicable, implement preventive measures
  - Document findings/lessons learned, actions, and outcomes
- Explain business continuity concepts
  - Fault tolerance
    - Replication
    - Redundancy
    - Backup considerations
    - Contingency plan
  - Disaster recovery
    - Data restoration
    - Prioritization
    - Restoring access