**RISK MANAGEMENT & BUSINESS CONTINUITY**

**ASSESSING RISKS**

In trying to understand risk management here are some terminologies we must assimilate

1. SLE – This means “Single Loss Expectancy”
2. ALE - This means “Annual Loss Expectancy”
3. ARO – This means “Annual Rate of Occurrence”

The total cost of a risk to an organization on an annual basis (ALE) is the Single loss expectancy multiplied by the Annual rate of occurrence.

The single loss expectancy is the financial loss that is expected when an adverse event occurs (e.g. a break-in which results in the loss of 2 of the most important servers, or the occurrence of a natural disaster, which could possibly affect business premises in more disaster prone regions).

ALE = SLE x ARO

To determine this, we must know the worth of each asset, the potential impact of that risk on the business and the likelihood of the threat/event.

We must then juxtapose the risk (ALE) against how much it would cost us to remove/alleviate the system vulnerabilities or implement repairs and get back online.

If our server is only prone to a scan from hackers from time to time, that means we might not consider hardening it since the cost of hardening the system or buying an already hardened one, eliminating those vulnerabilities might be financially draining compared to the risk; secondly since there are other things in place to protect it in the event of an attack – but we might still be prone to a scan from time to time.

If on the other hand a server room is at high risk of being hacked or experiencing a natural disaster/complete shutdown, we then use the potential financial loss that is expected from this specific adverse event (SLE) to determine how much damage it would do to the business if the disaster takes place. Hence since this would have more financial impact compared with the actual risk, we must have an alternate server perhaps in an alternate site we can switch operations to in the event of such an emergency. This is how we assess risks.

**MITIGATION STRATEGIES**

**Technical Controls** – These can be hardware and software installations which prevent threats and attacks to computer systems and services. They also monitor systems within the network for possible attacks e.g. firewalls, SIEMs, Anti-viruses etc.

**Management Controls** – Here we are monitoring adherence to the organization’s security policies. For example, to ensure security policy is effectively adhered to, a monthly security scan and audit for each department in an organization can be carried out and overseen by a cybersecurity team. This helps to ensure compliance to management’s standards.

**Operational Controls** – Here we are protecting our organization’s day to day operations to prevent key assets from being damaged. Example of things that can be implemented to ensure our organization’s day to day operations are not affected could include door locks, guards at entrances, motion detectors, security clearance access to restricted server rooms to avoid theft or data breaches etc. These are all operational controls. If there is a theft or an intruder, this could disrupt our daily operations.

**Loss Controls** – Also known as **“Damage controls”**, these are controls implemented which we make use of to protect key assets from being damaged. These controls may also reduce the severity of the loss when it occurs e.g. Sprinkler systems, fire extinguishers can be useful in reducing damage in the event of fire.

**DATA RECOVERY AND BUSINESS CONTINUITY**

When a breach occurs or a security incident, it is expected that this should not affect the business operations as this could eventually make it lose its customers. As a result, every business/organization should come up with a response strategy which should be incorporated into their official policy.

In that strategy, it should be determined how there would be internal & external communication during the incident, and the requirements for handling the incident.

Usually the organization should have already created an **Incident Response Team (IRT)** and prepared them with all the resources it needs to handle these possibilities. Concepts like redundancy, fault tolerance should be been in place while data recovery, switching to a new server/operational site and restoring critical business processes are all things to be implemented in response to such event by the IRT. All these are critical to business continuity.

**RECOVERING THE DATA**

Business continuity involves a process of securely recovering data and other sensitive resources in order to keep the business in operation. A trusted administrator can supervise the recovery process, documenting the steps and information that were used in the process. Secure backups must be done from time to time to prepare for this moment of recovery

**Full Backup**

All selected files regardless of their prior state are backed up.

**Differential Backup**

All selected files that have changed since the last full backup are backed up.

**Incremental Backup**

All selected files that have changed since the last full or most recent backup (incremental) are backed up.

Hence you have a new full backup different from the last full backup and most recent backup.

In such instance, we restore the last full backup plus all subsequent incremental backups since there may have been changes sequentially to these recent backups.

**ACRONIS CYBERPROTECT FOR SYSTEM AND DATA RECOVERY**

**Acronis Cyber Protect for System and Data Recovery – Beginner’s Guide**

1. Introduction

When learning about cybersecurity, one of the most important things to understand is how to protect systems and data against loss, damage, or attacks. Acronis Cyber Protect is a tool designed to help businesses and individuals secure their computers and quickly recover from disasters such as cyberattacks, accidental deletions, or hardware failures. It combines cybersecurity features with backup and recovery in one solution.

2. Why Data and System Recovery Matters

Data is valuable: Every organization relies on data (customer information, financial records, project files). Losing it can be devastating.

Threats are real: Cyberattacks like ransomware can lock or destroy files. Hardware can also fail unexpectedly.

Recovery is critical: Even with the best security, incidents happen. Being able to restore systems quickly ensures business continuity.

This is where Acronis Cyber Protect stands out—it not only tries to prevent problems but also ensures you can recover if they occur.

3. Key Features of Acronis Cyber Protect

a. Backup and Recovery

* Automatically creates copies of your entire system, applications, and files.
* Supports both full system recovery (restore your whole computer or server) and granular recovery (restore a single file or folder).
* Backup can be stored locally (external drives, servers) or in the Acronis Cloud, ensuring availability even if your physical system is destroyed.

b. Cybersecurity Protection

* Anti-malware and ransomware defense: Actively monitors your system and blocks attacks before they spread.
* Vulnerability assessments: Scans your system for outdated software or weak points hackers could exploit.
* Patch management: Helps keep software up to date automatically.

c. Disaster Recovery

* If a cyberattack or system crash occurs, you can boot your system from a secure backup.
* Provides bare-metal recovery, meaning you can restore a system onto a completely new machine if the old one fails.
* Allows remote recovery, which is especially useful for distributed teams or organizations.

d. Unified Management

* A single dashboard for IT teams to manage security and recovery across multiple devices.
* Simplifies monitoring, reducing the time spent switching between separate backup and antivirus tools.

4. How Beginners Should Understand this software

Think of Acronis Cyber Protect as a safety net:

* Prevention: It tries to stop cyber threats before they cause harm.
* Preparation: It creates secure copies of your system and data in case something goes wrong.
* Recovery: If disaster strikes, you can roll back to a safe state quickly and continue working.

**For example:**

1. If ransomware locks your laptop, you don’t have to pay the attacker. You simply restore your last clean backup.
2. If your hard drive fails, you can reinstall everything exactly as it was on a new drive.
3. If an employee accidentally deletes important files, you can recover them in minutes.

5. Benefits for Organizations and Individuals

* Reduced downtime: Systems are restored quickly, minimizing loss of productivity.
* Lower risk of data loss: Regular backups ensure critical files are always safe.
* All-in-one solution: Instead of buying separate antivirus and backup tools, you get both in one.
* Peace of mind: Knowing you have a reliable recovery option allows businesses to focus on growth.

6. Conclusion

* For beginners in cybersecurity, understanding Acronis Cyber Protect is a good way to grasp two core principles of cyber resilience:
* Protect before disaster strikes (through security and proactive backups).
* Recover quickly when disaster happens (through system and data restoration).

In simple terms: It’s like having both a strong lock on your doors (security) and a spare key plus a blueprint of your house (backup and recovery) in case something goes wrong.

Acronis Cyber Protect demonstrates how modern cybersecurity solutions are not just about defense but also about ensuring survival and continuity when things go wrong.