APAC Cybersecurity Fund

The Asia Foundation

Module 6

Protecting Your Business and Data with Backups

implemented in India by

Foundation for MSME Clusters (FMC)

with support from Google.org

Training Module developed under the project **APAC Cybersecurity Fund**

This training module is designed to provide general information and guidance on cybersecurity best practices. While every effort has been made to ensure the accuracy and relevance of the content, the information provided is for educational purposes only and does not constitute professional advice or an exhaustive cybersecurity strategy. By participating in this training, you acknowledge and accept that the information is provided "as is," without any guarantees or warranties of any kind, express or implied. For tailored cybersecurity solutions, please consult with certified experts.

Organized by **The Asia Foundation**

Implemented in India by **The Foundation for MSME Clusters**

Supported by **Google.org**

Module also available in Hindi, Marathi, Punjabi, Kannada and Telugu

Module developed by **Global Cyber Alliance** & **CyberPeace Foundation**

Module designed by **Chowdhury, Basu & Ray**

Version 1.0 December, 2024

Module 6

What We Will Talk About

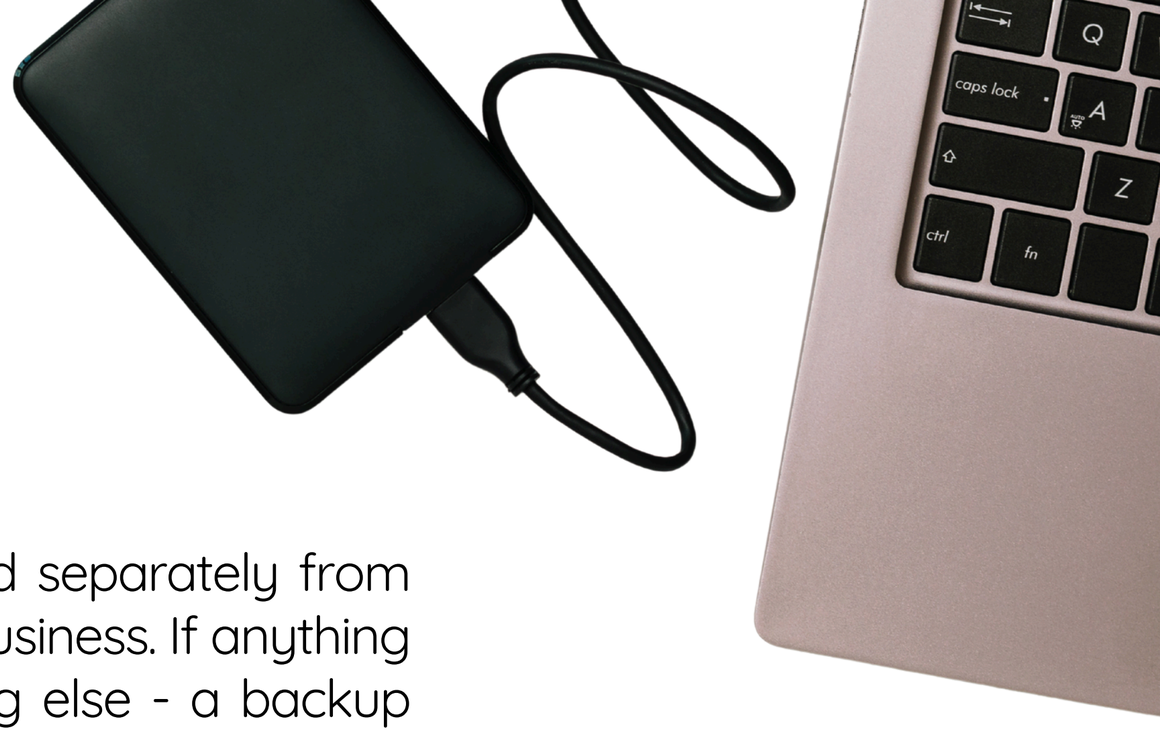
Business Continuity and Backups

As more information lives in digital form, backing up your data is critical from a business and personal perspective and crucial for business continuity. This is important no matter what type of device(s) you use: mobile, tablet, laptop, and/or desktop.

Modern reliance on mobile devices and computers means the impact of data loss or downtime can seriously impact or destroy an organization's productivity and profitability. Having backups is absolutely critical to being able to recover quickly and resume business operations after a loss.

Apart from ransomware attacks locking you out of your data, there are many other ways you can lose access to your data. While our focus here is preventing loss or corruption of data due to a cyberattack, backups also help with recovery from hard disc failure, equipment theft, human error, flood or accidental damage, and more.

1. BACKUP BASICS
2. DIFFERENT WAYS TO BACKUP YOUR DATA:
3. CONTINUITY PLANNING
4. DISASTER RECOVERY PLAN FOR YOUR MSME!
5. BACKUP AND RECOVERY CHECKLIST



Backup Basics

Backups are copies of key information or data stored separately from your device. Backups are absolutely critical for every business. If anything happens - cyber-attack, natural disaster, or something else - a backup allows you to quickly restore your data or device and get back to business quicker.

Data backups reduce recovery time, enabling MSMEs to restore operations quickly after disruptions, which is critical for MSMEs reliant on daily cash flow. Legal and financial implications can arise if data breaches, or loss of customer information occur. Backups can mitigate potential legal liabilities by preserving evidence of due diligence.

There are different ways to backup your data:

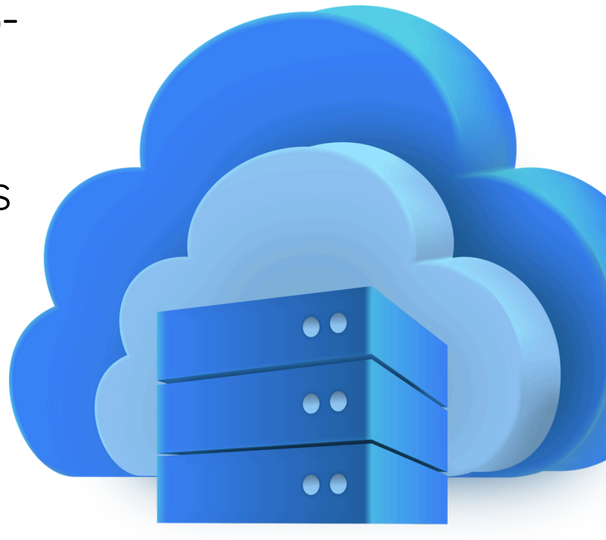
Offline Backup:

- Offline backup refers to data storage that's both local and offline, such as storage on an external hard drive, USB drive, memory card, or other device.
- These external devices should be disconnected and stored separately from the device itself.
- Store these devices in a safe and secure location. Take into account any environmental factors. For example, if you are in an area with high chances of flooding, store them on the second or third floor.
- Consider affordable external hard drives like Seagate or WD, with encryption features.

There are different ways to backup your data:

Online/Cloud Backups

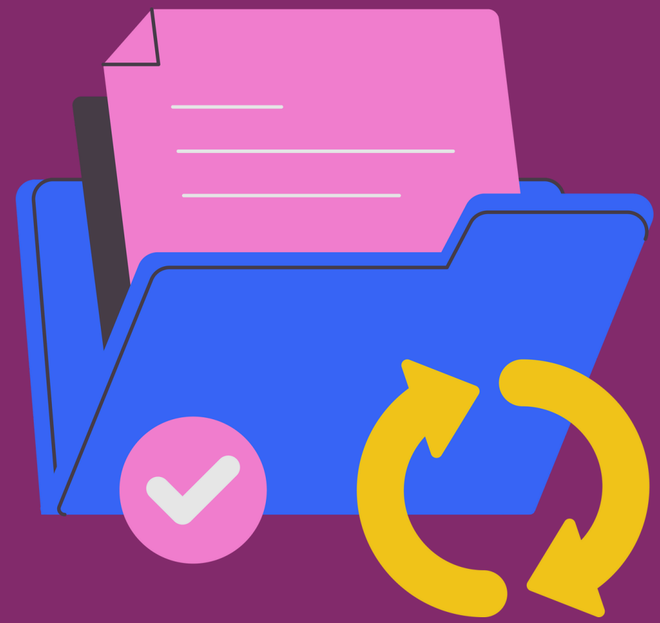
- Online backups create copies of your important data and store them off-site on secure servers 'in the cloud.'
- Online backups can be set to backup automatically at regular intervals and provide good recovery for many cases (such as theft or flood).
- Take into account the security of the cloud backup. Do they use encryption and two-factor authentication?
- Storing data on cloud platforms like Google Drive, Dropbox, or Microsoft OneDrive is recommended. Local options such as ZNetLive and Netmagic provide secure, cost-effective options for MSMEs.



Continuity Planning

Ensure you have a Disaster Recovery Plan, which helps recovery of critical systems following a disaster (whether accidental, natural, or malicious) and continuity of business operations. Having a plan helps minimize recovery time and damage to systems, helps limit potential liabilities, and can also improve security.

There are many templates and guides for developing a plan available online. Make sure you keep it updated, and conduct mock scenarios to exercise the plan and ensure everyone knows how to implement it. Assign specific employees to monitor and implement continuity plans during incidents.



Let us develop a Disaster Recovery Plan for your MSME!

Step 1: Identify Critical Assets

- Define Key Data and Resources: Make a list of all critical data (e.g., customer information, financial records) and resources (e.g., computers, servers) essential for business operations.
- Prioritize: Rank assets by importance. Focus on assets that would disrupt business significantly if lost.

Tip: For MSMEs, start with essentials like customer data, financial records, and operational processes.

Step 2: Conduct a Risk Assessment

- Identify Threats: List potential risks like cyberattacks, hardware failure, natural disasters, or human error.
- Assess Impact: Estimate the impact and likelihood of each risk on your business operations

Example: If a phishing attack is common in your sector, mark it as a high-priority risk

Let us develop a Disaster Recovery Plan for your MSME!

Step 3: Define Recovery Objectives

- Recovery Time Objective (RTO): Set a target time frame for restoring operations (e.g., within 24 hours of an incident).
- Recovery Point Objective (RPO): Determine the acceptable amount of data loss, typically measured in time (e.g., a few hours of data)

Step 4: Outline Backup Strategies

- Choose Backup Types: Select offline (external hard drives) and online (cloud) backup methods based on your RPO.
- Schedule Regular Backups: Set automatic daily or weekly backups for essential data.

Tip: For low-cost options, consider rotating external storage devices weekly.

Step 5: Develop an Incident Response Process

- Assign Roles: Identify key personnel responsible for specific tasks in a disaster recovery scenario.
- Create a Response Flowchart: Outline steps to take immediately after an incident, including reporting protocols, backup checks, and restoration processes.

Step 6: Create a Communication Plan

- Internal Communications: Decide how to inform employees during an incident and assign spokespersons for updates.
- External Communications: Plan how to notify clients, suppliers, and stakeholders if their data or services are affected.

Tip: Have templates ready for emails and messages to reduce response time.

Step 7: Document and Test the Plan

- Document Procedures: Write down each step, including details on accessing backups, contacting support, and restoring data.
- Run Simulations: Conduct drills quarterly to ensure staff are familiar with the plan and backup processes work smoothly.
- Update Regularly: Review and update the plan as your business evolves or as new risks emerge

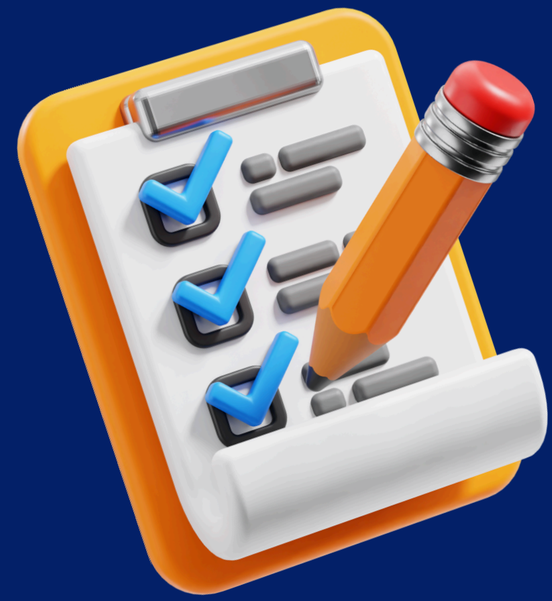
Backup and Recovery Checklist

Backup & Recovery Essentials

- Schedule automatic backups for high-priority data.
- Store backups in multiple locations (offline and cloud).
- Set up alerts to notify when backups are complete or fail.

Sector-specific Recovery Priorities Retail MSMEs

- Customer data, sales records, and inventory.
- Manufacturing MSMEs: Production data, supplier contacts, machinery configurations.
- Service MSMEs: Client data, project records, invoicing details.



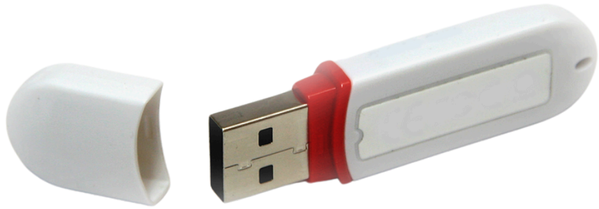
Protecting Your Business and Data with Backups

Backup and Recovery Checklist

Risk & Priority Mapping

- Identify all important data assets within the MSME, including customer information, financial records, intellectual property, and operational data
- Check for all probable attack sources, including phishing, malware, ransomware, data breaches, and accidental deletion.
- Check existing security measures and identify weaknesses like outdated OS, employee training, periodic security checks
- Calculate the impact of vulnerability exploits for each asset, using either a simple qualitative scale or a more quantitative approach.
- Create a prioritized list of risks based on their potential impact and likelihood.
- Develop Mitigation Strategies which may include updating security software, limiting access, improving physical security, and an established backup and recovery procedure

Backup and Recovery Checklist



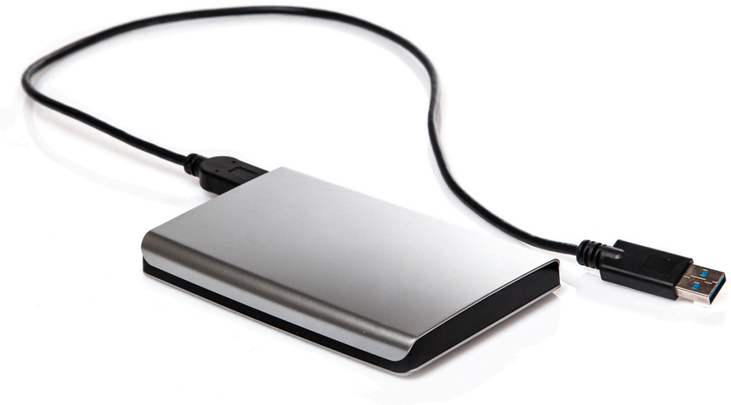
Map Data Based On Risk Categories

- Financial DataBank details, tax documents.
- Customer Data: Personal information, order history.
- Operational Protocols: Employee records, product details.

Google Drive

Low-cost Hardware & Other MSME-Friendly Solutions

- Basic external hard drives
- USB sticks for physical backups
- Budget-friendly cloud plans like G-Drive for online storage



Q&A Session

Any questions or thoughts?

Share with us your queries or thoughts

APAC Cybersecurity Fund

The Asia Foundation

Thank you for your attention!

For further assistance you can also reach out to the CyberPeace Foundation at helpline@cyberpeace.net or on WhatsApp at +91 957-00-000-66

Training Module developed under the project **APAC Cybersecurity Fund**

implemented in India by Foundation for MSME Clusters (FMC)

with support from Google.org