APAC Cybersecurity Fund

The Asia Foundation

Module 1

Understanding Cyber Risk for MSMEs in India

implemented in India by

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 1

Understanding Cyber Risk for MSMEs in India

Cyber-attacks target micro, small, and medium-sized enterprises (MSMEs) just as often as large ones, but MSMEs don’t often have teams or resources dedicated to actively protect against these attacks.

This course will teach you the basic protection measures your business against cybersecurity threats with the limited resources most MSMEs have at their disposal. It will show you how to reduce your cybersecurity risk level in practical ways that don’t require a lot of time, money, or expertise.

What We Will Talk About

1. CYBER RISK FOR MSMES: WHY IS IT SO IMPORTANT?
2. WHERE DOES CYBER RISK COME FROM?
3. FUNDAMENTALS OF CYBER HYGIENE
4. NEXT STEPS

Cyber Risk for MSMEs: Why is it so important?

‘Cyber risk’ indicates the probability that your business will suffer a loss. It can take many forms.

This can include financial loss, disruption to business operations through a hacked website or social media account, loss of critical data or personal information of employees or customers, as well as reputational damage. Protecting your business and managing your cyber risk needs to be part of your overall business operations and planning.

Cybersecurity for MSMEs helps to:

- Protect sensitive business information.
- Protect customer data.
- Build a trustworthy brand.
- Protect stakeholder interests.
- Avoid downtime
- Ensure business continuity.
- Achieve supply chain stability.
- Inspire partnerships.
- Protect financial information.
- Protect intellectual property.

Here’s why cybersecurity for MSMEs in India is relevant:

MSMEs in India represent 30% of GDP. According to the Ministry of MSME (2023), nearly 60% of Indian MSMEs have experienced cyber incidents but lack comprehensive cyber defenses. India has seen a 300% increase in cybercrimes against small businesses since 2021. -National Cyber Security Coordinator.

According to the DSCI, 43% of cyberattacks in India target small businesses. MSMEs face the same threats as large corporations but have fewer defenses. The urgency is heightened as India promotes digital adoption under the Digital India initiative. With MSMEs increasingly establishing online presences and integrating mobile-first technologies, they become primary targets for attackers who exploit limited cybersecurity frameworks.

Where does cyber risk come from?

There are 2 classifications of cyber risks:

- on the basis of **Origin** and
- on the basis of **Intent**

Cyber risk on basis of

Origin

- **Internal Risks**: Employee errors, unsecure Wi-Fi, weak passwords.
- **External Risks**: Phishing, ransomware, and malware attacks from third-party actors.

Cyber risk on basis of

Intent

- **Deliberate:** Ransomware, phishing.
- **Incidental/Accidental:** Employee accidentally opens a phishing email, uses a public Wi-Fi, has weak passwords. Incidental threats include cases where MSMEs that are dragged into a cyber incident that is actually targeting a larger corporation or as a result of some other incident like an unrelated data breach or a power outage creating system vulnerabilities.

Understanding Cyber Risk for MSMEs in India

When we talk about cyber crime, it is essential to remember that cyber criminals are organized. Today, most threats come from organized attempts to steal data to sell for financial gain and utilize a centrally controlled network of collaborators, each performing a specific function, creating a sophisticated hierarchy that is easily scalable and repeatable.

Cyber criminals will take advantage of any opportunity to exploit world events, regional disasters, and individual weaknesses for their own purposes and gain.

Internal threats can also be deliberate, originating from within the organization, often by employees or former employees. Malicious insiders are different from negligent insiders.

The business of cyberattacks:

Cybercriminals monetize successful attacks either by stealing data and directly selling it or by holding the data hostage and demanding ransoms (this approach is known as a ransomware attack).

Ransoms are an especially attractive revenue stream for hackers because this approach doesn’t require finding a buyer for the stolen data in the underground market. Ransoms are typically paid in more difficult to trace bitcoin, which most companies don’t have easy access to.

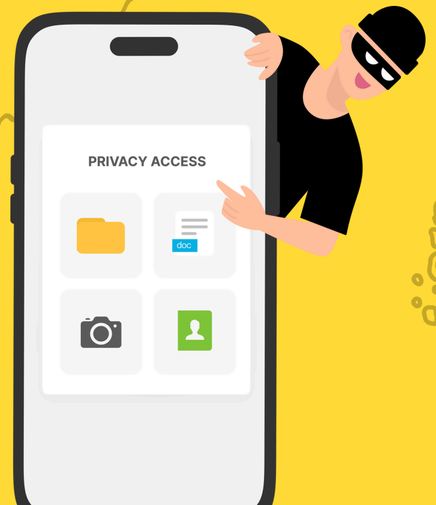
Cybercrime Market Players:

- **Sole Traders/Lone Wolves:** Operate alone or with a small handful of individuals to create and sell cyberattack products.
- **Organized Crime Groups:** Coordinated networks of highly sophisticated hackers, developers, and organizations who exploit and monetize the data they've stolen.
- **Marketplace:** Platforms for individuals and groups to buy and sell cyberattack products or services.
- **Supply Chain:** Network of creators, developers, and suppliers for cyberattack products and services.

Cyber criminals may not be targeting you or your business specifically!

- **Supply chain:** You may be targeted because they see your business as a potential route into a higher profile customer or partner of yours.
- **Outdated or pirated systems/software:** You may fall victim to an attack because of the systems or software you happen to be running.
- **User error:** You may fall victim to an attack because you or a member of your staff acted on a phishing email, unwittingly visited a malicious website, or accessed accounts via insecure Wi-Fi network.

Why MSMEs in India are prime targets?



As per Statista's report of Global Internet Access, India is a mobile-first nation, with over 1.05 billion internet users primarily accessing the internet through smartphones.

MSMEs primarily rely on mobile phones and digital tools for business operations. 95% of MSME transactions are mobile-based, making them prime targets for mobile-specific threats.

MSMEs are attractive targets due to lower security investments and high-value financial transactions. There are many reasons why your business could be a victim of cybercrime — understanding and reducing risks wherever you can make good business sense.

Interactive Session

Have you ever faced any cyber-threat ?

Share with us your experience

Understanding Cyber Risk for MSMEs in India

Managing Cyber Risk

With the increasing interconnectivity of all of our systems and devices, as well as changes in how we conduct business, security weak spots and vulnerabilities are growing exponentially.

Most MSMEs do not have the time or expertise to effectively address these on their own.

Challenges faced by MSMEs

MSMEs face some unique challenges when it comes to cybersecurity, owing to their scale of operations and the resources at their disposal. These include:

- Limited budgets.
- Cannot hire or contract specialized IT / cybersecurity personnel.
- Old devices.
- Legacy infrastructure.
- Outdated or pirated software.
- Lack of tech-savvy.

Implementing the most basic cyber hygiene practices can **prevent up to 86% of the most basic cyber-attacks**. Keep in mind that no matter what type of device you are using to support your business (mobile phone, tablet, laptop, and/or desktop) these same cyber hygiene steps apply.

Things you may be concerned about:

- It seems too hard.
- I don't have the time.
- I don't have the funds to pay someone to help me.
- I don't have the funds to buy tools to protect my business.

You are not alone! These are common and legitimate concerns. But this series of mini-courses is designed to give you a basic understanding of the steps you can take and the resources available to help you

Fundamentals of Cyber Hygeine

Leadership: Lead by example and educate your staff, volunteers, or family members who might also share your devices on the basics you learn here.

Know what you have: Keep an inventory of hardware and software that you use for your business. Deactivate devices (mobile, tablet, laptop, desktop, hotspots, etc.) or accounts you no longer use.

Software updates: Do them right away and automate all the ones that you can. Software systems that are not up-to-date with the latest security patches are one of the biggest risk factors to your business.

Backups: Consistently backup your data and keep multiple copies off-premise and with a secure cloud solution.

Passwords and tools to protect them: Create unique and strong passwords for each account. Use two-factor authentication and password managers for added security.

Access control: Not everyone needs access to everything or the same privileges. Limit users and permissions to only what they need. This includes the ability to download **new software or apps.**

Remember that cybersecurity is for ALL members in an organization and not limited to any one department or team. If every person in the organization is aware of good cyber hygiene, there are fewer opportunities for cybercriminals to gain unauthorized access.

As you develop strong cyber hygiene habits, here is **a quick checklist** of common mistakes to avoid:

- Don’t use default or easily guessable passwords, and avoid password reuse across accounts.
- Don’t leave systems and software unpatched, as vulnerabilities can be exploited by attackers.
- Don’t open untrusted or suspicious emails, attachments, or links, as they may contain malware.
- Don’t store sensitive data or passwords in plain text or unencrypted formats.
- Don’t grant excessive privileges or access rights to users beyond what is necessary.
- Don’t neglect physical security measures, such as access controls and secure disposal of sensitive data.
- Don’t disable or bypass security controls, such as firewalls, antivirus software, or IPS/IDS systems.
- Don’t connect untrusted or unauthorized devices to your network.
- Don’t share sensitive information or credentials over unsecured channels or public networks.
- Don't ignore security alerts, warnings, or suspicious activities, and promptly investigate and respond.

Before we jump into the courses, here's a **quick action plan** to keep handy in case you're ever hit by a cyber attack in India:

- Call the national Indian Cyber Crime Helpline at 1930.
- Report to CERT-In: Notify the relevant authorities for mandatory reporting. Report on the cybercrime.gov.in portal
- Lodge a complaint at your local police station / cyber cell.
- Identify the incident: Determine if it's a data breach, ransomware, or phishing attack.
- Contain the damage: Disconnect affected systems to prevent spread.
- Notify stakeholders: Maintain transparency to uphold trust with customers, funders-donors, partners, service providers and the relevant authorities.
- Prepare for larger communication in the event of media involvement. Choose if you want to release a social media statement at every stage.
- Restore from backups: Ensure regular backups to minimize operational downtime.
- Review and improve cybersecurity measures: Learn from the incident to strengthen defenses.
- Ask an external expert or auditor to gauge your response and recovery efforts.

Q&A Session

Any questions or thoughts?

Share with us your queries or thoughts before we proceed to Module 2

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