

A paradise of structured learning...

## Cyber Security in wake of Covid -19 Pandemic



# Contents :

- ✚ Introduction
- ✚ Cyber Security WHY??????
- ✚ What is Cyber Security ?
- ✚ Elements of Cyber Security
- ✚ Cyber Security Threats
- ✚ Cyber Crime Infographics
- ✚ Cyber Security Threats to be aware of in 2020
- ✚ Ways to Prevent Cyber Attacks
- ✚ Cyber Security Hygiene – A Way forward while in WFH Mode
- ✚ 10 Best & Worst Prepared Countries for Cyber Crime
- ✚ Top 10 Biggest Data Breaches of All Time



# Introduction:

---

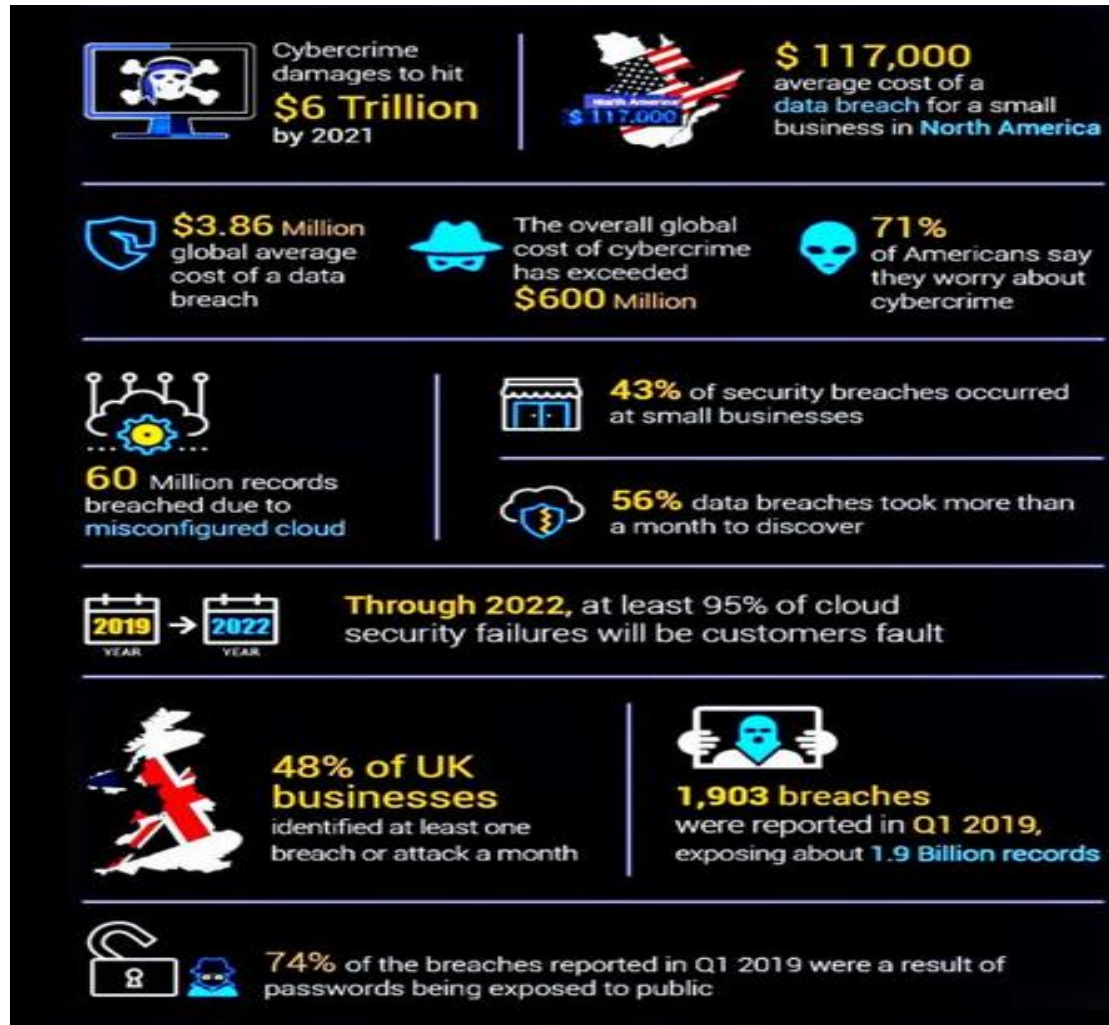


The coronavirus outbreak has sent the world into a complete chaos. The COVID-19 pandemic has, almost overnight, forced us to adapt to a whole new working environment. After nearly five months in quarantine, both organizations and employees have come to terms with working remotely or working from home.

While we may have converted a part of our home into a workplace, it is important to remember that we are now using our home network to connect to global servers and downloading more data it normally expects and cybercriminals will be quick to exploit this opportunity. Malware, scams, and phishing attacks related to the COVID-19 crisis are all on the rise, as are cyberattacks on healthcare providers. With millions of people working and learning from home, the world is moving online at an unprecedented rate – and so is cybercrime.

How, then, can we ensure that our devices and our networks are more secure? It has been observed that, while consumers today are more aware than before of cybercrimes, data breaches, and online threats such as phishing, the measures they adopt for cyber security may often not be adequate. With remote working likely to become a more common feature of corporate work culture in the lockdown period, we need to be better prepared to ward off cyber threats.

# Cyber Security WHY??????



<https://icssindia.in/>

# What is Cyber Security ?:



# SCCE

Cyber security may also be referred to as information technology security. Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. It is also known as information technology security or electronic information security.

Cyber security is important because government, military, corporate, financial and medical organizations collect, process and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences.

Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation's top intelligence officials cautioned that cyber attacks and digital spying are the top threats to national security, eclipsing even terrorism.

As quoted by , research firm Canalys, Worldwide Cyber security spending is estimated to grow between 2.5 % - 5.6 % percent in 2020 as threats and vulnerabilities persist for organisations, and the shift to remote working during lockdown makes it important for enterprises to invest in extending perimeter defences.



# Elements of Cyber Security:

Strong cyber security on a systematic approach include the following :

- **Application Security** : Applications play an essential role in business ventures; that is why every firm needs to focus on web application security. Having a secure web application is required to protect customers, their interests and their assets. Web application weakness or vulnerabilities is a common point of interference for a cyber thief.
- **Information Security** : Information includes business records, personal data, customer's data, and intellectual property. For an organization, it is vital to have strong Cyber security for information as it is the heart of every organization.
- **Network Security** : Network security consists of protecting the usability and reliability of network and data. A network penetration test is conducted to assess the vulnerabilities in a system and other security issues which occur in servers, hosts, devices and network services.



# Elements of Cyber Security: (Contd....)

---

## ➤ **Disaster Recovery:**

- ❑ **Business Continuity Planning** : Business continuity planning (BCP) is all about being prepared for interference or cyber threat by identifying threats to the organization on time and analyzing how operations may be affected and how to overcome that.
- ❑ **Operational Security** : Operations security (OPSEC) is used to protect organization functions. It tracks critical information and assets to identify vulnerabilities that exist in the functional method.

- **End-user Compliance** : One of the standard errors that lead to data breaches is human error. Organization Cyber security is kept as strong as the weakest link. It is vital for an organization to train their employees about Cyber security. Every employee should be aware of the phishing attacks through emails and links and should have the potential to deal with cyber threats they may face. The employee should share their device password with their co-workers and should not use an insecure network.

To have a successful Cyber security project, it is vital to have leadership commitment. Without having the leadership in the team it is complicated to develop, implement and maintain the processes. The top leaders or management team an organization should invest in the Cyber security measures to make it useful and successful. With the support of leadership for Cyber security, an organization can improve investment in technology, resources, and skills.

# Cyber Security Threats:

The risk and severity of cyber-attacks have clearly grown over the past few years. In fact, since the year 2018, mankind has witnessed the most horrific cases of cybercrimes related to massive data breaches, flaws in microchips, cryptojacking, and many others.

It goes without saying that the advancement of technology and the wide use of digital media is making attackers smarter by the day. Further, these cybercriminals take advantage of individuals and firms who pay less heed to Cyber security. They target everything from a newly-launched blog to an established online store to gain access to sensitive information.

Every other day we read news related to Cyber security threats like ransomware, phishing, or IoT-based attacks. However, 2020 comes with a whole new level of Cyber security threats that businesses need to be aware of. In fact, a report by Threat Horizon reveals that in the coming years, organizations will face cyber threats under three key themes –

- **Disruption:** Over-dependence on fragile connectivity will increase the risk of premeditated internet outages that compromise business operations. Cybercriminals will use ransomware to hijack the Internet of Things.
- **Distortion:** Spread of misinformation by bots and automated sources will cause compromise of trust in the integrity of information.
- **Deterioration:** Rapid advances in smart technologies and conflicting demands posed by evolving national security will negatively impact an enterprise's ability to control information.



# Cyber Crime Infographics :

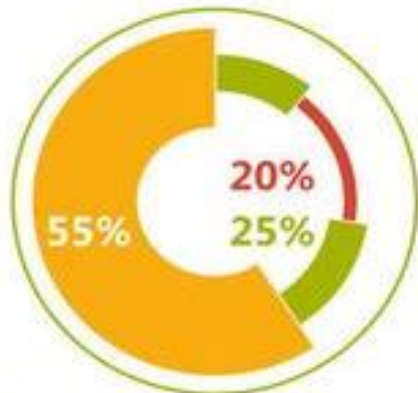


## METHODS OF PROTECTION FROM CYBERCRIME



## QUANTITY ATTACKS

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium,



unde omnis iste natus error sit voluptatem



## 35% TROJAN HORSE

>Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut

## 18% DNS FLOOD

>Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore

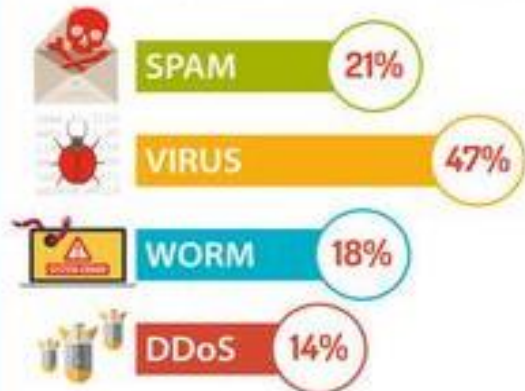


## 47% PHI-SHING

>Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore



## TYPES NETWORK ATTACKS



Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore ventratis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit

# Cyber Security Threats to be aware of in 2020 :

---



1. **Cloud Vulnerability** : The Oracle and KPMG Cloud Threat Report 2019 reveals that cloud vulnerability is and will continue to be one of the biggest Cyber security challenges faced by organizations. This is because enterprises are leveraging cloud applications and storing sensitive data related to their employees and business operations on the cloud.
2. **AI-Enhanced Cyberthreats** : AI and Machine Learning have disrupted every industry. Owing to its ability to create a significant impact on marketing services, manufacturing, security, supply chain management, and other fields, AI is finding its way into the business mainstream. However, AI is proving to be a boon for cybercriminals too. The AI capabilities used to identify and stop cyberattacks can also be used by hackers to launch sophisticated cyberattacks in the form of complex and adaptive malicious software. In fact, AI Fuzzing (AIF) and Machine Learning (ML) poisoning are all set to be the next big Cyber security threats.
3. **AI Fuzzing** : AI fuzzing integrates AI with traditional fuzzing techniques to create a tool that detects system vulnerabilities. This can be a boon or a bane. Though AI fuzzing can help enterprises detect and fix the exploitable vulnerabilities in their system, it can also be used by cybercriminals to start, automate, and accelerate zero-day attacks.
4. **Machine Learning Poisoning** : If a hacker targets a Machine Learning model and injects instructions into it, the system becomes vulnerable to attacks. Machine Learning models typically use data that is crowd-sourced or taken from social media. They also exploit user-generated information such as satisfaction ratings, purchasing histories, or web traffic. Cybercriminals engaging in ML poisoning could potentially use malicious samples or introduce backdoors or Trojans to poison training sets and compromise the system.

# Cyber security Threats to Be Aware of in 2020 : (Contd....)



5. **Smart Contract Hacking** : Though smart contracts are in their early stages of development, businesses are using them to execute some form of digital asset exchange or the other. In fact, it's smart contracts that make Ethereum famous. Smart contracts are software programs that carry self-executing code. This code enables developers to create the rules and processes that build a blockchain-based application. Consequently, these contracts are a prime target of online criminals looking to compromise such applications. Moreover, since it is a brand new field, technologists are just about getting to know how to design them and security researchers are still finding bugs in some of them. These vulnerabilities make it easy for criminals to hack the contracts. As this technology continues to mature, smart contract hacking will pose a significant threat to businesses in 2020 and beyond.
6. **Social Engineering Attacks** : Social engineering attacks like phishing have always been used by attackers to trick victims into surrendering sensitive information like login details and credit card information. Though most organizations are enhancing their email security to block phishing attacks, cybercriminals are coming up with sophisticated phishing kits that aid in data breaches and financial fraud. Since phishing is an effective, high-reward, and minimal-investment strategy for cybercriminals to gain legitimate access to credentials, it will continue to be a big Cyber security threat in 2020. SMiShing (SMS phishing) is another form of social engineering attack that will gain prominence in the near future. The immense popularity of apps like WhatsApp, Slack, Skype, WeChat, and Signal among others is encouraging attackers to switch to these messaging platforms to trick users into downloading malware on their phones.
7. **Deepfake** : First coined by Reddit users in 2017, 'deepfake' is a fake video or audio recording that cybercriminals use for illicit purposes. For instance, amateurs and criminals have created deepfakes by swapping people's faces in videos or altering its audio track.

# Ways to Prevent Cyber Attacks:

---

Cyber Attacks on businesses seems to be inevitable- at least with the prevailing situation in the cyber landscape. But security analysts say that to a large extent most of these attacks are avoidable if companies choose to follow the below-specified steps crafted specifically to protect their enterprises against cyber attacks.

- To have a secure and sophisticated hardware which are password protected and backed up by 2-way authentication.
- **Safeguard your company's hardware** - Most of the data breaches occur when stolen equipment reaches the hands of the hackers. Thus, it's better to outline some physical security strategies before any untoward incident occurs. Like storing the data on the cloud which is protected by multiple security layers and inculcating responsible security policies among the employees working for your business environment.
- **Encrypt data** - Encryption of data gives your company an upper hand when your data falls into wrong hands. And that's due to the fact that it becomes useless even if a hacker sniffs it out- and mind you it's not that easy to break into the encryption available in the market these days.
- **Backup data** - Sometimes no matter how hard you try, hackers get into your network and try to encrypt your data with ransomware. But if your enterprise has a backup copy of the latest, then you or your company need not bow to the demands of the hackers. The backup should be done in an effective manner and that too should be in the retrievable form as soon as a disaster strikes.
- Educate employees on the latest happening in the cyber landscape, so that they can help mitigate cyber risks with ease. This includes educating them about risks associated with using unsecured networks to access work info and avoiding unsecured websites and sharing sensitive data on social media. Restricting them from password sharing will also help.
- Use of anti-malware solutions and protecting enterprise networks with efficient firewalls will also help in keeping your enterprise IT safe from attacks.

# Cyber Security Hygiene – A Way forward while in WFH Mode:

---



With exponentially more people working remotely, and with the likely increase in the use of cloud-based services, more than ever before we have to stress the importance of employing good cyber hygiene and discipline.

Remember, many people are working remotely now who have never worked remotely before. They may not be aware of things they are doing that can inadvertently create unnecessary risks. Among the basics that must be communicated:

- When working remotely, keep business and personal accounts separate. The bleed over of risk from personal to business can be detrimental to a company or a government organization.
- Use best practices in basic hygiene such as using strong passwords and changing them routinely, and using multi-factor authentication, identity management and device security settings.
- Make sure users know what to do if a device is lost, stolen or compromised. Make sure IT and security teams have the proper tools for monitoring and visibility across cloud environments.
- Apply the same principles in the cloud as you would on premises—including decisions about what is most important to protect, prioritizing resources and having the ability to see and stop threats that pose the greatest risks to your core mission.

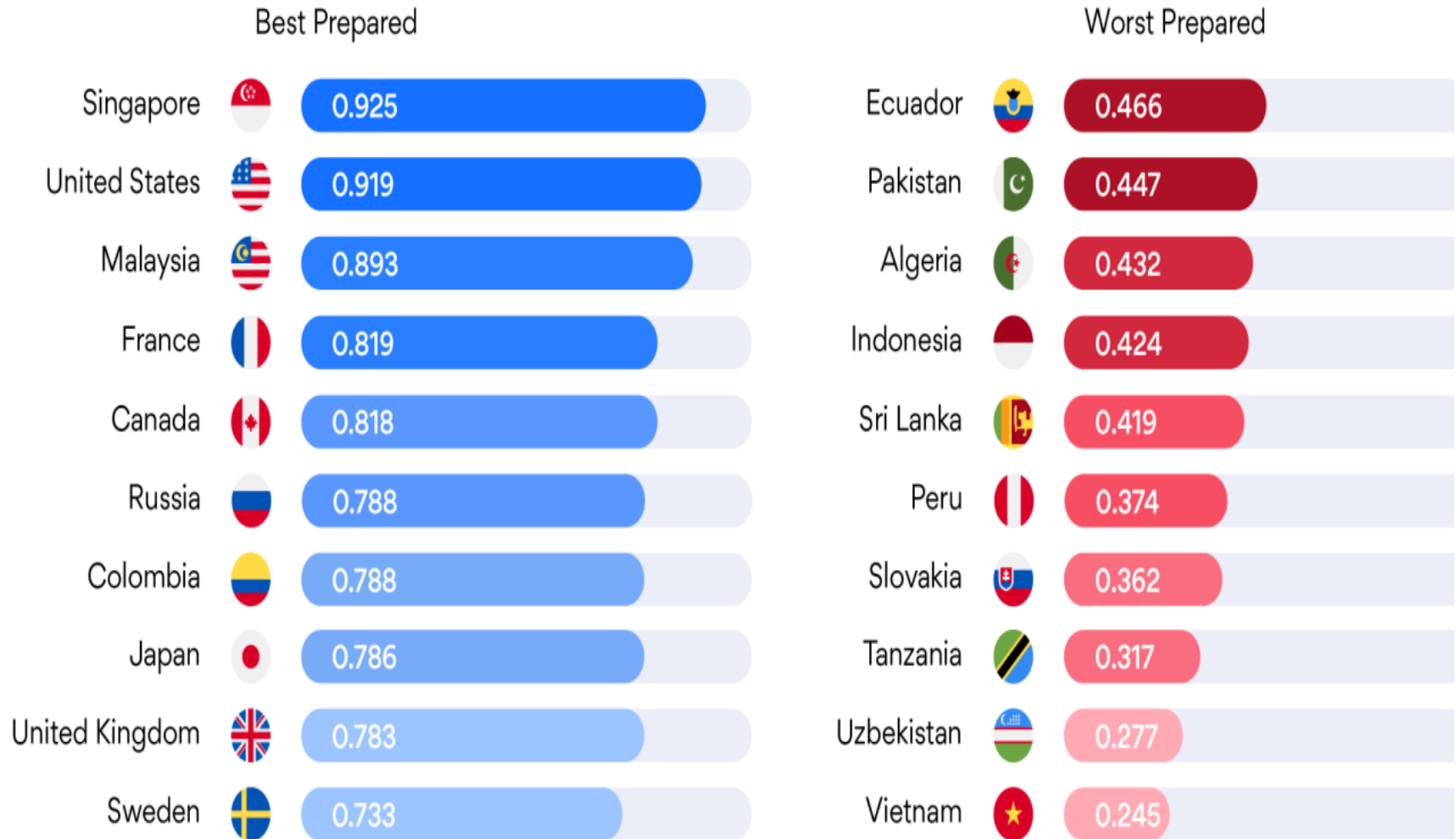
Most of all, it's very important to try to keep things as simple as possible. In an environment of uncertainty, keep complexity at bay.



# 10 Best & Worst Prepared Countries for Cyber Crime:

























































# SCCE



<https://uk.pcmag.com/>

## Top 10 Biggest Data Breaches of All Time :

	Company	# of ppl affected	What got leaked
1	 COURT SQUARE VENTURES	200 million 	names  addresses  bank details 
2	 U.S. VOTE FOUNDATION	191 million 	 birth dates  phone numbers  party affiliations 
3	 Adobe	150 million 	e-mail  password  credit card details 
4	 ebay	145 million 	    
5	 Heartland	130 million 	credit card details 
6	 TARGET	110 million 	     
7	 T.K. maxx	94 million 	credit card details 
8	 Anthem	88 million 	   social security numbers  employment information 
9	 PlayStation	77 million 	names  addresses  e-mail  birth dates 
10	 MOSSACK X FONSECA	11.5 million 	11.5 million leaked documents  214 000 offshore companies 

<https://www.le-vpn.com/>

# Sources of Information :



# SCCE

- <https://www.netsparker.com/>
- <https://indianexpress.com/>
- <https://digitalguardian.com/>
- <https://yourstory.com/>
- <https://www.infoguardsecurity.com>
- <https://www.computer.org/>
- <https://uk.pcmag.com/>
- <https://www.Cyber security-insiders.com/>
- <https://www.securityroundtable.org/>
- <https://twitter.com/>

If you have liked reading this issue or have any suggestions for improvements, please do write to the team : [cascade@scce.edu.in](mailto:cascade@scce.edu.in), [sccecascade@scce.edu.in](mailto:sccecascade@scce.edu.in) or [cascade\\_scce@scce.edu.in](mailto:cascade_scce@scce.edu.in)

Cascade, a monthly electronic publication of SCCE is distributed by SCCE, Pune with an access to all the Corporate Learners. This is also for the benefit of our alumni and due care has been taken to ensure that the information published herein is correct to the best of our knowledge.

**Website:** [www.scce.edu.in](http://www.scce.edu.in)

**Email:** [cascade@scce.edu.in](mailto:cascade@scce.edu.in) ; [sccecascade@scce.edu.in](mailto:sccecascade@scce.edu.in) ; [cascade\\_scce@scce.edu.in](mailto:cascade_scce@scce.edu.in)

**SCCE, Pune - Cascade Team : Dr. Seema Singh, Director, SCCE, Pune and Ms. Mayura Pathak, Supervisor, SCCE, Pune**