simplilearn

An Introduction to

Cyber Security

A Beginner's Guide

TABLE OF CONTENTS

INTRODUCTION

The belief that "it will not affect us" is the biggest blunder that a modern-day organization can make on the issue of cybersecurity. The cybersecurity threat is real, and it is, now, a worldwide problem.

In this digital era, every organization, be it SMEs or large corporations, governments or banks, faces the threat of a system hack, ransomware attack, data breach, or malware. Cyber-criminals of today are not old-time lone hackers. They run organized crime networks and often operate like startup companies, hiring highly-trained programmers to innovate new online attacks.

With organizations having to secure an increasing amount of sensitive data, cybersecurity is becoming relevant and essential for businesses of all sizes. As the scale and scope of threats continue to rise at a fast pace, fresh opportunities are opening up for qualified data professionals in diverse sectors.

While Gartner predicted that the international cybersecurity market will reach US$ 170.4 billion by 2022, IDC forecasts US$ 133.7 billion global spending on security solutions in the same year.

Experts believe that the proliferation of IoT-connected devices, cloud-based applications, a range of technology initiatives, and strict privacy protection mandates are driving the rapid growth of the cyber security market.

Cybersecurity is undoubtedly one of the fastest-growing fields. However, there is an acute shortage of skilled workforce. If you are enthusiastic about securing organizational digital assets but are unsure if a cyber security career is right for you, the **basics of cyber security handbooks** will clear your doubts.

Starting with **cyber security introduction**, this **cyber security handbook** will discuss everything you should know about cybersecurity threats, the worst affected sectors, security analytics use cases, cyber security terminologies, and the skills in demand.

AN OVERVIEW OF CYBER SECURITY

Cyber Security is a set of processes, technologies, and methods to protect servers, computers, networks, electronic systems, data, and mobile devices from unauthorized access through malicious attacks.

Securing the availability, confidentiality, and integrity of an organization's digital assets and software against internal or external threats is the primary objective of cyber security.

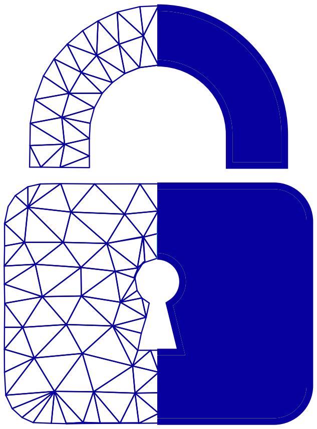
The term cybersecurity encompasses a wide variety of security solutions. Common cybersecurity categories include -

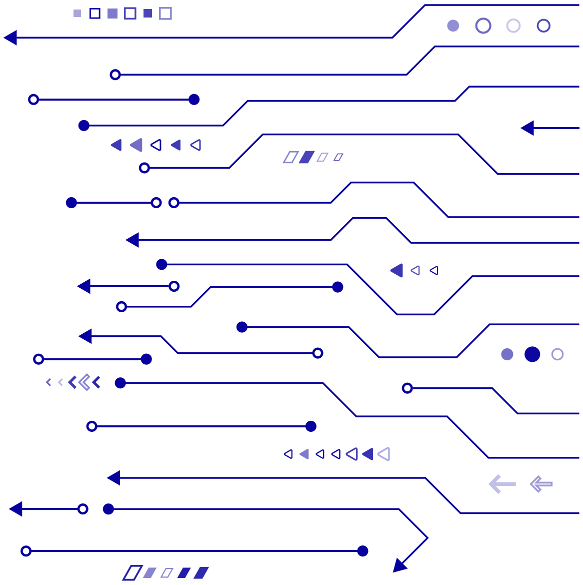
- ✓ **Application Security:** Compromised applications can facilitate unauthorized access to data. Application security protects devices, applications, and software from cyber-attacks.
- ✓ **Operational Security:** From access permissions to decisions and processes that determine where and how data will be shared or stored, fall under operational security. It places a great emphasis on securing data assets.
- ✓ **Information Security:** All about protecting the privacy and integrity of data in transit and in storage.
- ✓ **Network Security:** The process of ensuring security to computer networks from opportunistic malware or targeted attackers.
- ✓ **End-user Education:** This cybersecurity category covers an extremely unpredictable factor—humans. End-user education aims to teach users about cyber security threats and the best security practices to avoid them.

CYBER THREAT EXAMPLES

Cybersecurity solutions protect against three types of cyber threats, which are—

- **Cyber Attack:** Unauthorized information gathering.
- **Cyber Crime:** Groups or single actors targeting systems, networks, or servers for monetary benefit or for causing disruption.
- **Cyber Terrorism:** Undermines electronic system to cause fear or panic.





THREATS THAT CHALLENGE CYBERSECURITY

The methods used by cyber attackers, criminals, or cyber terrorists to gain control over an organization’s computer system include —

- **Malware**

  Malware is malicious software. Hackers or cyber criminals create malware to damage or disrupt computer systems. Criminals also use malware to launch cyberattacks or to extract money.

  Viruses, Spyware, Trojans, Adware, Botnets, and Ransomware, are common instances of malware.

- **Phishing**

  Phishing targets its victims through authentic-looking bank or company emails, asking for confidential data, such as personal information or credit card details.

- **Man-in-the-Middle Attack**

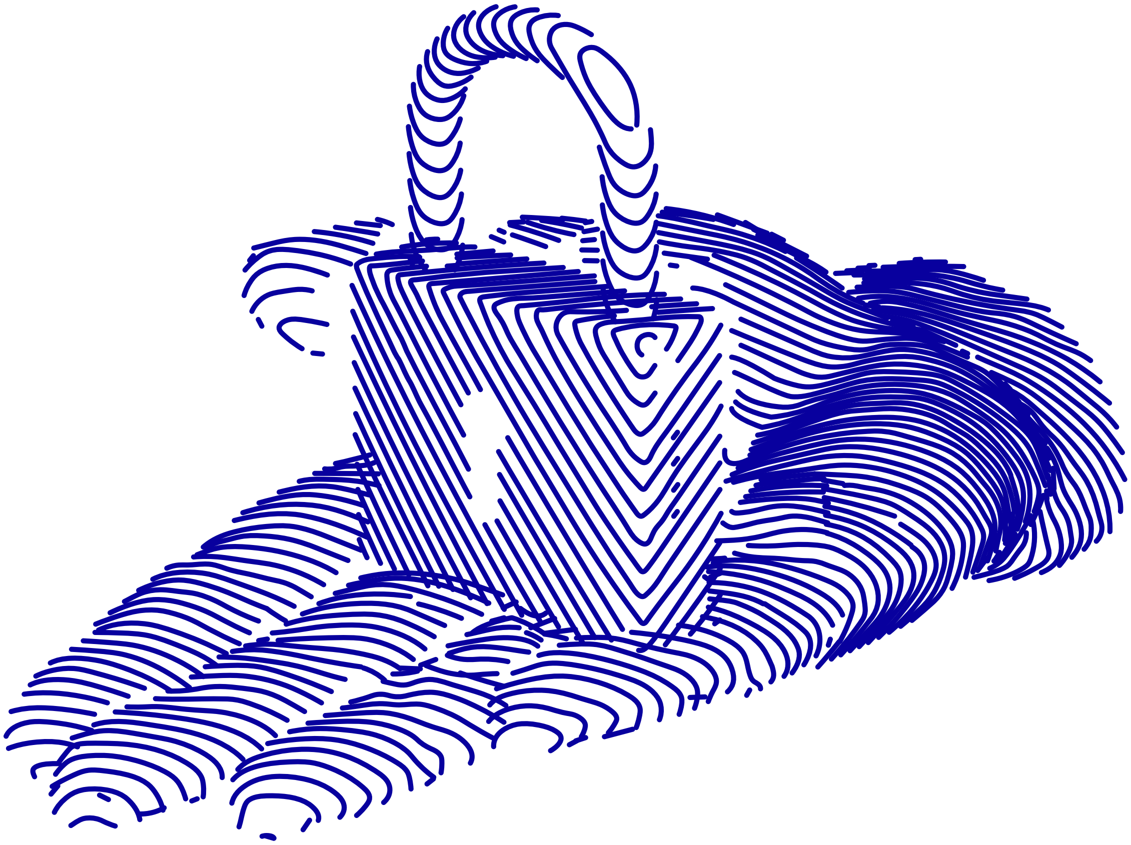
  In a man-in-the-middle attack, internet criminals intercept communication between 2 individuals for stealing data. Cybercriminals carry out these attacks on unsecured networks.

✓ Denial-of-Service Attack

This attack overwhelms servers and networks with traffic overload, denying computer systems from completing legitimate requests.

✓ SQL Injection

Cybercriminals use a Structured Language Query (SQL) injection to gain control over databases. This gives attackers access to sensitive data stored in databases.



INDUSTRIES THAT HAVE A HIGH CYBERSECURITY RISK

The Theft Resource Center identified 780 data breaches across different industries in 2015, which left 169 million personal data or records at risk.

Since then, security pros detected several hacking incidents, and now it is no secret that the following industries are more vulnerable to security risks.

Health Care

From AI to VR, voice search to the blockchain, and chatbots, the healthcare industry is introducing innovative technologies to boost patient care. These advanced technologies improve the quality of life, but unfortunately, because of them, cybercriminals are increasingly targeting the sector. Hackers exploit the medical industry to obtain important patient data available in clinics and hospitals, such as patient bank details, social security numbers, and personal addresses.

Manufacturing

Thanks to the Internet of Things and cloud technologies, the manufacturing sector has become more efficient in communicating with customers and supply chains. However, connected technologies bring with them multiple access points that allow cybercriminals to steal factory and customer data.

Retail

Retail faces a constant cyber threat because of the huge transaction volume that takes place within the sector every day. Internet scammers target the retail industry to pick credit card details, online account data, and other customers' personal information.

Finance

In 2015, cybercriminals hacked into the multinational credit reporting organization Experian PLC, a brokerage company Scottrade, and the American stock market index, Dow Jones. Even in 2020, there were reports of hacking into PayPal accounts, Australian banks, and banks in Southeast Asia. For understandable reasons, financial institutions are at the forefront of cyber-attacks.

Use Cases of Security Analytics

Security Analytics is a cybersecurity approach that collects and analyzes data from diverse network sources to create proactive protection measures. With this knowledge, security analytics solutions produce actionable insights by automating threat hunting. There are three use cases of security analytics, which include -

✓ Real-Time Analytics

Real-time analytics analyzes alerts coming from real-time security systems such as SIEM (Security Information and Event Management). For example, it can detect dangerous Internet Protocol addresses in real-time, based on known threat patterns and severity.

✓ Rule-Based Analytics

Drawing intelligence feeds on existing and potential threats, rule-based analytics defines and applies rule-based approaches to identify and counter known attacks or bad actors.

Batch Analytics

Unlike real-time and rule-based, batch analytics analyzes unknown attacks. It uses data profiling and statistical models to identify threats. Batch analytics can also facilitate the visualization of security vulnerabilities.

Cyber Security Applications

Combining the above three security analytics models, cybersecurity provides the following solutions.

Cloud Monitoring

The cloud presents unique challenges when IT scales. Cybersecurity ensures tight supervision of the cloud infrastructure and cloud-based applications.

Behavior Analysis

Users continuously interact with an IT infrastructure, and their behavior determines the failure or success of an organization's security. Cybersecurity analytics monitors users for unusual behavior to detect malicious activities, insider threats, and compromised accounts.

Network Analysis

Traffic moves out and comes into the network all the time. However, because of the high volume, maintaining visibility over every network transaction is not possible. Rule-based security analytics provides network cybersecurity by setting standards and criteria.

Data Extrusion Detection

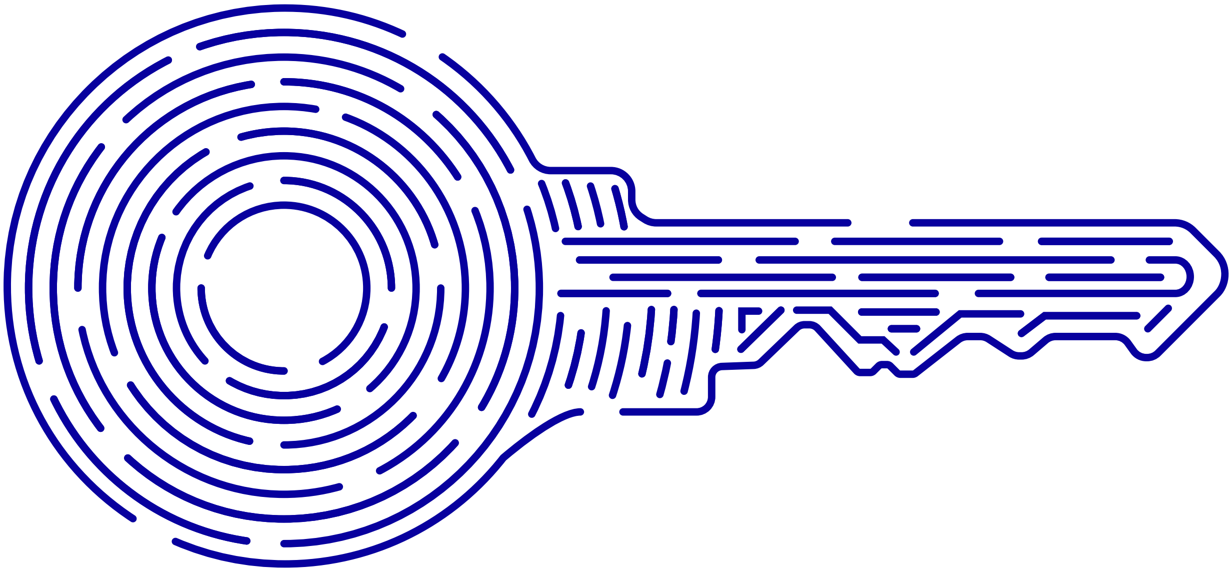
Data extrusion or data exfiltration refers to unauthorized data transfer from computers. The transfer can be via physical access, or automated, through malware. Unsanctioned data movement can lead to data leakages and theft. Cybersecurity, using security analytics, can identify data exfiltration and prevent data theft.

Insider Threat Detection

An insider threat, caused by a careless, malicious, or ignorant user, can be as damaging as an external threat. Insider threats, sometimes, can wreck a network. Cybersecurity analytics can detect insider threats by analyzing user behavior, such as unusual login times, abnormal email usage, and unauthorized access requests.

Threat Hunting

Simply responding to threats puts organizations in a tight corner. Cybersecurity automates threat hunting, which enables continuous scanning for dwelling threats and potential breaches. This implements a comprehensive and proactive protection measure.



A QUICK GLOSSARY OF CYBER SECURITY TERMINOLOGIES

- ✓ **Access -** Gaining control over a system's information or knowledge.
- ✓ **Adversary -** An individual or a group with criminal intent.
- ✓ **Antivirus -** A software that protects a computer from a malicious attack.
- ✓ **Asset -** Documents, information, resources, and other data that are of great importance.
- ✓ **Backdoor -** Instant access to a system without the need to log in.
- ✓ **Botnet -** Compromised or infected devices on an internet-connected network.
- ✓ **BYOD (Bring Your Own Device) -** Employees bringing and using their own devices, authorized by an organization.
- ✓ **Cloud Computing -** On-demand availability of system resources, typically computing power and data storage without a user's active or direct management.
- ✓ **Ciphertext -** A plaintext encrypted with an encryption algorithm.
- ✓ **Confidentiality -** The state of keeping something private or secret.
- ✓ **Cyber Essentials -** Industry-supported, Government-backed policies to help protect organizations against online threats.
- ✓ **Data Breach -** The unintentional or intentional release of private or secure information.
- ✓ **Decode -** To convert an encoded message into comprehensible language.

- **DoS (Denial of Service) -** A cyber-attack that disrupts services by denying access to network resources or machines.

- **Exfiltration -** Transfer of data without consent.

- **Ethernet -** The architecture for interconnecting computer systems via a wired local area network.

- **EUD (End-user device) -** A device capable of storing information, such as a PC, laptop, smartphone, tablet, hard drive, memory card, or USB flash drive.

- **Exploit -** An attempt to breach secure networks to gain access to digital assets.

- **Forensics -** An application of analysis and investigation to gather evidence from computing devices.

- **Firewall -** A security system that controls and monitors outgoing and incoming network traffic in conformity with predetermined rules.

- **GDPR -** General Data Protection Regulation – a law that regulates how organizations protect the personal data of EU citizens.

- **Hacker -** A cybercriminal who uses electronic devices to obtain unauthorized data access.

- **Hashing -** An algorithm applied to data to validate that the information is not corrupted, tampered, or modified.

- **ISO 27001 -** A globally recognized standard for risk management of information security as per the ISMS (Information Security Management System) procedures and policies. ISO 27001 accreditation proves to stakeholders and clients that an organization is managing information security effectively.

- **ICT (Information and Communications Technology) -** An extended term for IT, stresses unified communications, such as the integration of computers, mobile phones, wireless networks, the internet, middleware, enterprise software, and media applications.

- **Integrity -** This refers to data that has not been tampered or modified.

- **Jailbreak -** A process of removing device security restrictions, allowing its user to make modifications.

- **Keystroke Logging -** Also called keylogging, it refers to capturing a computer user's keystrokes on a keyboard.

- **Logic Bomb -** A code inserted to set off malicious functions in software systems.

- **Macro Virus -** A virus programmed in the macro language. Microsoft Excel and Word are common applications featuring macro languages.

- **Malware -** Malicious software designed for disrupting, damaging, or gaining unauthorized access.

- **Network -** Connected computers linked through the internet.

- **NIS Directive -** A European Union directive on the security of information systems and networks.

- **NIST Cybersecurity Standard -** National Institute of Standards and Technology (NIST) guidelines for US private enterprises to follow for improved detection and response to cyber-attacks.

- **Outsider Threat -** An external security threat by a group or an individual.

- **Penetration Testing -** Often referred to as ethical hacking, it is a simulated cyber-attack to assess a system's security.

- **Phishing -** A fraudulent and criminal attempt to obtain sensitive information by disguising as a legitimate entity.

- **Quadrant -** Technology for making tamper-proof cryptographic equipment

- **Ransomware -** Malicious software that disrupts a system and demands a ransom to make it workable again.

- **SaaS (Software as a Service) -** A software delivery model on the cloud on a subscription basis.

- **Security Perimeter -** A boundary between networks with necessary safeguards against cyber-attacks.

- **Steganography -** A technique used to conceal data within ordinary messages and files to bypass detection.

- **Two-Factor Authentication -** An authentication mechanism that grants system access to a user only after presenting two authorization evidence.

- **Unsigned Data -** A data type that holds positive values.

- **Virus -** A malicious program that replicates on infected computers.

- **Worm -** A malware type that spreads its copies from one computer to another.

- **Zero-Day -** An unaddressed or unknown software vulnerability.

BUILDING A CAREER IN CYBERSECURITY

Cyber Security Skills to Land a Job

To pursue a career in cybersecurity, you must have a range of skills, including technical, operational, management, and communications. Here is a list of the basic skills you will need to enter the world of cyber defense.

✓ Problem Solving

Solving critical problems will be part of your daily work. You will need to be innovative in creating effective measures to address complex security challenges.

✓ Technical Aptitude

As a cybersecurity professional, you need to be technologically savvy to keep up with current and emerging threats. You must keep in mind that the work of a cybersecurity expert is purely technology-focused.

✓ Familiarity With Multiple Platforms

Cybersecurity is not restricted to computers. It also protects wireless networks, cloud infrastructure, and handheld devices. So, being familiar with various platforms is essential.

✓ Attention to Details

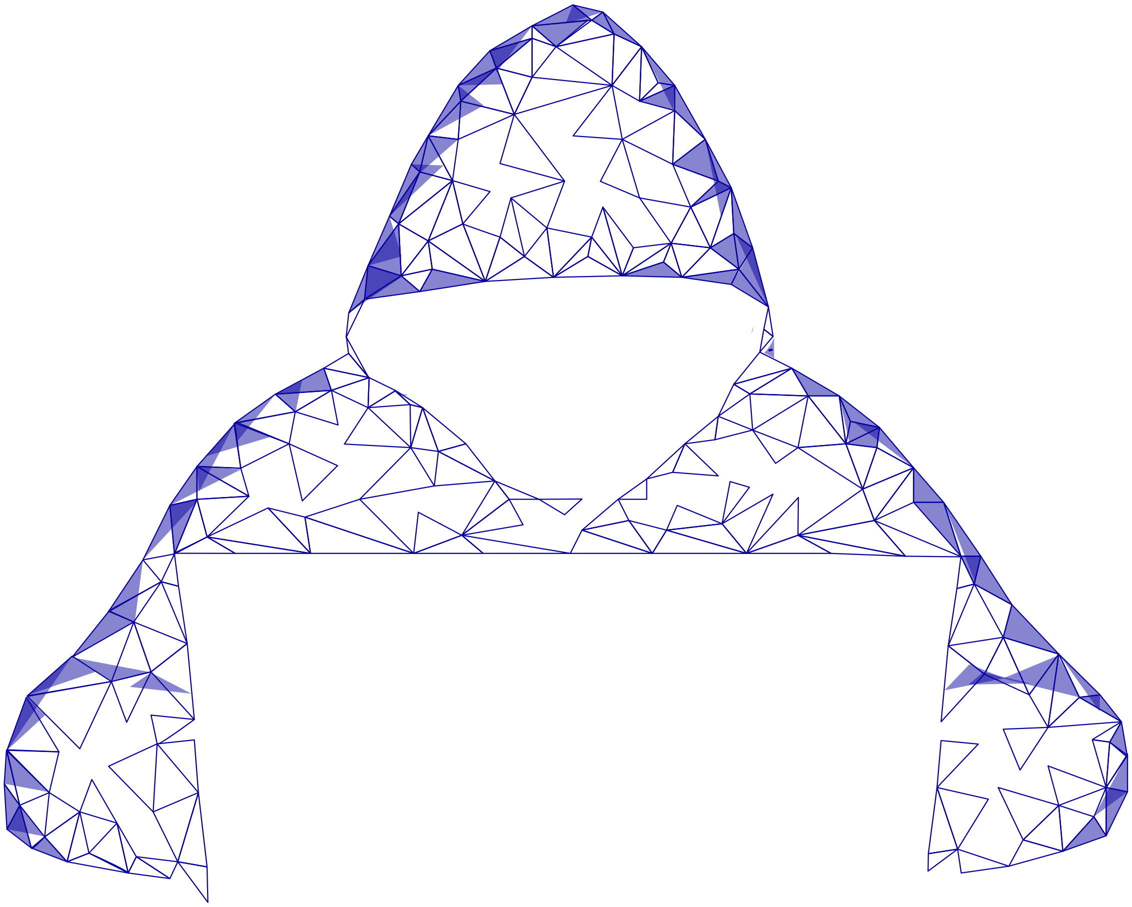
To secure large organizations from cyber-attacks, you need to be alert and attentive to details. As a cybersecurity professional, you will need to monitor the network 24/7, and if a threat occurs, you have to identify it swiftly and come up with security solutions in real-time. Therefore, staying attentive is vital.

Communication Skills

From Management to Chief Security Officer, vendors, and the general workforce, cybersecurity professionals must interact with every stakeholder. Having powerful communication skills is critical to effectively communicate security policies, concerns, and solutions to all.

Forensics Skills

While cybersecurity and computer forensics are two unique areas, they are, however, interrelated. Knowledge of computer forensics is necessary to understand what went wrong if your defense mechanism does not work. It also helps recover compromised data.



GET READY TO LAUNCH YOUR CAREER IN CYBER SECURITY

The field of cyber security is at the cusp of a real revolution, and the focus on related technologies, ideas, and practices are going to increase multifold in the near future. Businesses are looking for enthusiastic cyber security professionals who don't just have the basic skills but can think differently, respond to business challenges proactively, and innovate constantly.

Although a bachelor's degree in computer science is a good start, specialized training on the latest techniques, tools, and practices are critical to position yourself as a competent cyber security professional capable of supporting the current and future enterprise challenges.

Simplilearn, one of the world's top digital skills providers, offers multiple programs focussed on the most in-demand, and emerging technologies should be your first choice. The Cyber Security Master's Program from Simplilearn offers learners a comprehensive program that not only covers the fundamentals of cybersecurity but addresses the best practices and most effective cyber security techniques used today. The Master's programs also include multiple projects, quizzes, and assignments based on practical, real-world applications, helping learners become work-ready from the day they complete the program.

Other cybersecurity programs include;

- ✓ **Cyber Security Certification Course**
- ✓ **Certified Ethical Hacking Course**
- ✓ **CISSP Certification**
- ✓ **CISA Certification**
- ✓ **CCSP Certification**
- ✓ **CompTIA Security+ Certification**
- ✓ **COBIT® 2019 Certification Training**

Contact us to **learn more.**

simplilearn

INDIA

Simplilearn Solutions Pvt Ltd.

# 53/1 C, Manoj Arcade, 24th Main,
Harlkunte
2nd Sector, HSR Layout
Bangalore - 560102

Call us at: 1800-212-7688

USA

Simplilearn Americas, Inc.

201 Spear Street, Suite 1100,
San Francisco, CA 94105
United States

Phone No: +1-844-532-7688

www.simplilearn.com