Security and Compliance

A Must-Have Visual Guide

Niharika Srivastav and Sanjay Saxena

First paperback edition March 2023
ISBN: 979-8-3753-2654-2

CyberEdx

www.cyberedx.com

Advance Reactions

“Educating everyone on Cybersecurity is a must at this day and age. This book does an exceptional job of explaining complex topics in terms that are relatable and consumable for its target audience. It provides a solid foundation on theory while also sharing actual applications. I highly recommend this book!!”

- *Mica Syjuco, Director, Technology Leadership, Avanade*

“I highly recommend this book to anyone who wants to learn more about Cybersecurity. Kudos to Niharika and Sanjay for taking the initiative to write this book and spread cybersecurity awareness, to help the world become a safer place. A “must-read” book for all ages, everyone should have this book in their library.”

- *David Meece, Cybersecurity Professional, Passionate Cyber Mentor, International Speaker*

“Cybersecurity awareness is critical to securing organizations on a path of accelerated digital adoption. The book eliminates the complexity of the subject and blends the principles of program management and security in an *easy-to-understand* manner. The book provides a good combination of the theory as well as practical tips from real-life projects. A "must-read" for the business leaders to set them up for success.”

- *Ashish Agarwal, Former CIO, Indigo Airlines*

“This is an excellent book regarding cybersecurity and compliance. An easy read and digest on the basic understanding of frameworks to manage risk, compliance, and projects. It is a great book to add to your library. If you don’t know where to start concerning cybersecurity and compliance, start by reading this book! You will understand and be able to speak the basic language of cybersecurity and what to expect and look out for regarding security and compliance! Everyone needs to read this.”

- *Janet Tsai, IT Auditor, Aerospace Industry*

“Kudos to Niharika and Sanjay for simplifying the security jargon for the business leaders with the wonderful illustrations. This book comes at an ideal time, as global leaders take stringent steps to improve their countries' cybersecurity posture.”

- *Ajay Bhutoria, Book Author, Founder, Global Business Consulting*

“I found it to be a great introduction to cybersecurity and the cybersecurity mindset. Engaging and filled with tips, overviews and reinforcing exercises. I would highly recommend this to anyone interested in incorporating the fundamentals of cybersecurity into their methodology.”

- *Charles Hale, President, Hale Consulting*

"The fundamental concepts of complex information security and data privacy topics have been broken down into simple-to-understand language, with illustrations and actionable steps that could be readily consumed and applied to any project from inception through to delivery. A great reference point for delivery leads to ensure the secure delivery of their projects."

- *Vishal Garg, CISSP, Cybersecurity Consultant and Solution Designer*

"Cybersecurity, Data Privacy, and Compliance awareness is highly critical these days in any project/program from startup to well-established enterprises. I appreciate Niharika and Sanjay adopting a *process-centric* approach. Care has been taken to unpack the security concepts with simple and real-world examples. Very positive that the examples, exercises, scenarios will help guide the delivery teams."

- *Sri Srinivasa, Program Management Leader, Podcaster, Public Speaker*

"I was impressed with the vast knowledge of Cybersecurity composed and organized in an *easy-to-grasp* manner. I appreciate the dedication and effort of this book's writing, graphics, and editing team. I wish them success with the book and its adoption by project, functional, and business leaders. Last but not the least, I love *Chapter 10: Action Plan.* It makes the learning from the book easy to follow. Well done."

- *Sanjay Mathur, Founder, Frictionless Security*

"I liked this book. People who want to learn how cybersecurity is now an essential part of any project, as well as key concepts in cybersecurity, should read this book. I love the *simple way* very important topics of user identity and account security are covered. This book has nice *illustrations* and examples that are covered in an intuitive manner."

- *Nehal Mehta, President & Co-founder, Rainbow Secure*

"Cybersecurity is imperative for enterprises as well as nations today. With the proliferation of the digital lifestyle, rising Cybercrime and Cyber Warfare threats, it behooves all of us to be prepared. It is an easy-to-read Cybersecurity primer for leaders that helps address the enablement problem 'With so much at stake, how could we equip ourselves better?"

- *Piyush Malik, Chief Digital Officer, Veridic Solutions (Formerly Worldwide Big Data Analytics CoE Leader at IBM)*

"This is a comprehensive collection, of very relevant aspects of an increasingly important subject like Cybersecurity. I am sure delivery teams will find this *very handy*. It's an easy read (I presume by design) peppered with real-life experience and wrapped up with an *actionable framework* that can deliver tangible results."

- *Kanak Choudhary, Managing Director, Accenture*

Acknowledgements

Many thanks to Scott Cook, Co-Founder and Chair of Executive Committee at Intuit, who generously advised us to design the book for the READER'S DELIGHT. Special thanks to the experts who reviewed our drafts and suggested hundreds of changes that made the book more relevant and useful for the readers:

- J.L. Erskine, Retired Navy Veteran, Cybersecurity Instructor
- Bill Keyser, Retired Veteran, Cybersecurity Advisor
- Pari Vijay, Chief Growth Officer, Learnow.live
- Gene Libov, President, Planet9 Inc.
- Maria Leone, Senior Manager, Blue Shield of California
- Mindy Bergstrom, Sr. Director, Blue Shield of California
- Manohar Bijor, Entrepreneur, QA Expert
- Tanuja Singh, Technology Leader, Cisco
- Balu Nair, Client Services Leader – Healthcare, Infosys
- Sudhir Reddy Rebala, Ashtral Biotech Pvt. Ltd.
- Pratul Kant, Head of InfoSec, Metropolitan Transportation Commission
- Giles Hinchliff, Sr. IT Leader, Kaiser Permanente
- Alka Agarwal, Program Leader, Blue Shield of California
- Ranbir Bhutani, Security Consultant
- Florindo Gallicchio, VP, Strategic Solutions, NetSPI
- Swetha Mudunuri, Cloud Security Specialist
- Anav Batra, Product Manager
- Shikha Garg, Sr. Product Manager, Microsoft
- Amit Sheth, Sr. Director, Kaiser Permanente
- Satyan Mishra, CEO, Drishtee Foundation
- Akhilesh Singh, Group Senior Manager (IT), NHPC
- Helay Rahimi, Program Leader
- Varsha Vinod, CS Student, University of California

We would like to give our thanks to Shambhavi Johri, Piya Mitra, Alka Agarwal, and Nishi Agrawal for help with the cover design. Special thanks to Jay Parekh, Soumita Das for assisting with the diagrams, and Akul Saxena, for editing the draft.

Despite all of the reviews and feedback we've received on various parts of the book, we anticipate that this work will definitely not be perfect and that errors will be discovered after publication. If you notice any errors, please let us know at info@cyberedx.com

About the Authors

Niharika Srivastav

TOGAF, PMP is the SVP of Cybersecurity and Executive Programs at WITI (Women in Technology International). Niharika pursued her education at the Delhi College of Engineering, an MBA from the Delhi School of Economics, and an Executive Leadership Program from Stanford. Niharika has 25+ years of experience in engineering, projects/portfolio delivery, customer success, marketing, and sales. She is the board member of American Society of Engineers of Indian Origin, Silicon Valley.

Sanjay Saxena

CISSP, PMP, and Harvard Alumnus is the founder of CyberEdx, a platform focused on simplifying cybersecurity for non-techies. He pursued Engineering from SATI India and Post-Graduation from Harvard Business School. Sanjay has 25+ years of experience in enterprise architecture, program delivery, security, sales, and marketing. He hosts "*Hattrick with Sanjay*", a national radio show on Cricket. He has hosted radio shows on technology in the past. He is also a Sports Executive, working to promote Cricket in the USA.

About the Editors

Michael Gnoinski

Over the past 20 years, Michael has been active with the design, deployment, and management of technology to make large, long-distance running events like the Houston, Chicago, and Boston marathons function successfully. Michael, as an IT Project Manager, guide, and coach who successfully executed technology transitions and new deployment projects across the US.

Isabel Hinchliff

Isabel is a freelance editor and undergraduate student at the University of California, Berkeley. She is double majoring in English and Cognitive Science, with a minor in Creative Writing. She is a managing editor at Berkeley Fiction Review and a staff editor at PEP HAUS Magazine. In her free time, she likes to cook gluten-free food, writes dark speculative fiction, and reviews short stories for SFFreviews.com

Dedication

This book is dedicated to my late parents, Usha Shekhar and C.S. Prasad, who inspired me to pursue my dreams, my siblings Vineeta-Vivek, Richa-Ashutosh, my aunts and uncles Nitu-late Shashi, Kiran-Himanshu, Chitra-Subhash, to my mentors/colleagues Elinor Mackinnon, Lisa Gonzales-Simon, Alice Raia, Giles Hinchliff, Keith Kim, Ramdas Kharat, Rucha Nanavati, Sreelatha Vijayalakshmi, Sarath Sasikumar, Ravi Srivastava, Sandeep Vasukuttan, Gene Libov, Mike Wolfe, Tim Kerimbekov, Chad Aronson, Nina Barley, Supal Patel, Ram Gautam, Ram Patange, Jaynul Dewani, Vinay Sharma, Santosh Maila, and Aaron Rozek for their support and guidance.

To Sameer Mehta and Vijay Srinivasan of Major League Cricket for the opportunity to write professionally for 'The Times of India'. To the late BN Yugandhar, my father's coach during his tenure at the Academy of Administration, Mussoorie, India, for his inspiration.

- Niharika Srivastav

I dedicate this book to my late father, Chandra Shekhar Saxena, and my loving mother, Sudha, my siblings Alka-Vijay, Aruna-Rajendra, Shilpa-Sandip, my uncles Subhash & Arun Hajela, aunts Swaraj & Pratibha Hajela, Saroj Devi Saxena for encouraging me to venture beyond my comfort zone. To Vickrant Mahajan with 30+ Guinness World Records, a motivational coach to Olympic athletes, who motivated me to write books. To Prem Suri, Suraj Viswanathan, and Neeraj Dhar for their continuous support.

To my hero, Ken Rutwoski, founder of the fantastic community METAL, who inspires me every week with his thought leadership and interviews with world-class personalities. To Rajesh Setty, Adam Gilad, Kevin McMahon, Justin Bookey, Steve Rubin, Allen Mostow, David Richman, David Leighton, Freddie Ravel, Sam Morris, Neil Cannon, Dr. Mark Gouston, and the fellow METAL members for their encouragement and support during the book writing process.

To Tony Robbins (Business Mastery Program), David Rogier (Founder of Masterclass), and Vishen Lakhiani (founder of Mindvalley) for their creative ways to teach things and inspiring me.

-Sanjay Saxena

Table of Contents

Foreword

First of all, it is an honor to write a foreword for a book addressing such an important topic of cybersecurity. The mindset that cybersecurity is the responsibility of the company CISO has changed and the realization that cybersecurity is everyone's responsibility is pervasive in a modern enterprise.

Having said that, I don't always see people acting that way and most still depend on the CISO organization to lead the way.

The siloed nature of today's security disciplines is quickly becoming a liability as attackers are becoming more sophisticated and relentlessly targeting anything of value in the enterprise. Today cyber risk is identified as one of the top sources of risk for board members closely followed by regulatory and compliance risks. If it is top priority for the board, it is a top priority for the CEO and hence for everyone in the organization.

Security is no longer a 'nice to have', in fact security, privacy and compliance by design, are quickly becoming the building blocks of any important project, in other words security and compliance cannot be an afterthought. It has to be baked into the projects from the very beginning. This is where we see a lot of challenges because more often than not the project teams don't have the knowledge or the skills to do this.

Many project managers and even IT leaders still happen to think that security is the responsibility of other people – software architects, InfoSec specialists, and so forth. The truth is that it is a project team's task to ensure that the products they create or services they deliver are secure. Let me be clear, I don't expect the project leaders to become security experts overnight, but I do expect them to ask important questions related to security, privacy, and compliance such as:

- How are we minimizing the attack surface?
- Are we following the principles of assigning least privilege?
- Are we in compliance with the security policies laid out by the CISO?
- What security controls are we implementing?
- What separation of duties are we putting in place?
- How will we handle the right to be forgotten for GDPR and CCPA?
- What secure defaults are being established and what security frameworks are we following?

The first step to empowering leaders to ask these (and many other) questions is through basic security, privacy and compliance training and I am so glad that Niharika and Sanjay have taken it upon themselves to write this book to impart these skills. If you are a product or program manager or an IT or business leader, and you can master the art of driving secure practices for your projects or products, you will stand out from the rest. This book is a great way to get you started on the journey. Being a very visual person, it is wonderful to see so many wonderful illustrations which make complex concepts easier to understand. This book is a must read for you and for your entire team so let us empower ourselves with enough knowledge about cybersecurity to make the right choices at every step of our journey.

Sameer Khera

CIO, Norton Lifelock

Preface

The risk of cybersecurity threats certainly isn't new, but in recent times it has become an increasingly prominent issue. Cyberattacks have had massive impacts on the societal, political, and economic world in recent times.

Do you recall traveling to the airport to pick up someone prior to 9/11? [1] I remember walking up to the aircraft door when picking up and dropping off my friends. Even though I was not the traveler sometimes, I was allowed to proceed to the boarding gate until the flight was ready to depart. There were no security lines at any stage before boarding the flight.

Figure 1: Stringent security inspections and screenings at airports

Now, after 9/11, the number of security inspections and screenings at airports have dramatically increased. You must arrive at the airport at least two hours before your flight is scheduled to depart, go through a tough security screening, take off your shoes, belt, remove your computers, and whatnot from your luggage, and walk through a metal detector. There are several security cameras monitoring your every movement.

[1] The fatal day of September 11th, 2001

Have you ever found yourself in a situation where you were carrying something that wasn't allowed in your carry-on luggage? You probably had to toss the item away or return it to the check-in counter at the airport to check it in.

Similarly, when we first started designing internet applications, we didn't have to worry about writing security-related code, installing anti-malware, creating secure infrastructure, etc. But then, there were some huge cyberattacks and data breaches that transformed the entire digital world.

In recent years, there have been several attacks and breaches. A few recent examples:

- In January 2023, **T-Mobile**, a telecommunications company, discovered a major data breach, involving 37 million customers' names, birth dates, and phone numbers. The hacker gained unauthorized access to T-Mobile servers containing customer data.[2]
- In September 2022, **Uber**, the rideshare company, was breached, and sensitive user data was stolen. The hacker, posing as a trustworthy individual, obtained the credentials for an employee's slack account and gained access to cloud-based systems containing sensitive customer and financial information.
- In April 2022**, Oil India Limited** (OIL), the second-largest oil and gas company of India, had all the computers locked out after a ransomware attack. The group behind the cyberattack sought $7.5 million in Bitcoin to restore access.
- In May 2021, **Colonial Pipeline**, the largest gas pipeline in the United States, was hit by a ransomware attack. The pipeline was shut down, resulting in gasoline shortages across the East Coast. The hackers got away with a ransom of about $4.2 million.[3]
- In late 2020, **SolarWinds**, a third-party software supplier, was breached by hackers, who were able to attach malicious software to SolarWinds software updates. This allowed the hackers to actively monitor the internal operations of over 200 organizations worldwide, including many US government agencies.[4]
- In March 2020, **Brno Hospital**, one of the major COVID-19 testing facilities in the Czech Republic, was targeted by ransomware. As the computer virus spread, the hospital's systems began to fail, prompting management to shut down all

[2] https://www.fiercewireless.com/operators/t-mobile-ceo-says-hacker-used-brute-force-attacks-to-breach-it-servers
[3] https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

[4]news.bloomberglaw.com/privacy-and-data-security/solarwinds-hack-reached-27-u-s-attorneys-offices-justice-says

equipment. The hospital had to reschedule appointments, postpone operations, and even transfer patients to other hospitals.

Figure 2: Recent cyberattacks and breaches

These are only a few of the worst and most infamous attacks. The list of cyberattacks in recent years is long, and it is growing every day. According to the world's leading Cybersecurity researcher, Cybersecurity Ventures, Global cybercrime costs will grow by 15% each year over the next five years, it will reach $10.5 trillion USD per year.[5]

To combat the attacks, US President Joe Biden has taken a number of steps. In May 2021, he signed an Executive Order to improve the nation's cybersecurity and protect federal government networks.[6] In March 2022, he issued a warning to the American business leaders of Russian cyberattacks, telling them to strengthen their companies' cyber defenses immediately. In March 2023, the Biden administration released the National Cybersecurity Strategy to secure a safe digital ecosystem for all Americans. Leaders of other nations are also prioritizing cybersecurity as a central part of their national security initiatives.

To ensure that businesses use processes and procedures to secure their assets, various laws and regulations have been enacted. If the laws and regulations are not followed, fines are imposed. Regulations include GDPR (Global Data Protection Regulation), a

[5] https://securityboulevard.com/2021/03/cybercrime-to-cost-over-10-trillion-by-2025/
[6] whitehouse.gov

law enacted in the European Union (EU) to protect its citizens' personal data, HIPAA (Health Insurance Portability and Accountability Act), a US healthcare law which protects patients' sensitive data, and several other regulations. Companies and their employees must abide by all applicable laws, regulations, standards, and ethical practices in their organization, industry, and country. This is known as **compliance**.

To comply with regulations and secure assets, businesses are focusing on strengthening their security teams. As a result, there is a significant shortage of highly sought-after cybersecurity professionals. The number of unfilled cybersecurity jobs increased globally by 350% over an eight-year period, from one million in 2013 to 3.5 million in 2021, according to Cybersecurity Ventures.

Cybersecurity has become everyone's responsibility, whether they are cybersecurity professionals or not, to keep the organization safe. You may think that you already have a lot on your plate, and now you have to worry about security. However, you will find it easier if you are familiar with cybersecurity.

Figure 3: You must prioritize security

Whether you work for a startup or a large corporation, it is critical that you equip yourself with cybersecurity knowledge in order to drive secure practices in your organization. Let's begin our journey!

Introduction

Figure 4: A data breach example

Data breaches and cyberattacks are all too common these days and businesses are making headlines for not taking security seriously. There is an urgent need for security education at all levels of organizations. It is, however, easier said than done.

Over the course of our combined 50-year career, we've worked with and trained professionals ranging from entry-level to senior executives in a variety of industries. One common complaint we've heard is that there is a wealth of security information available on the internet, but it's difficult to decide what to pursue. Some of the information is either overly condensed or overly technical, making it difficult to follow.

We decided to simplify and organize this information in the form of a book *with illustrations and practical tips from real-life examples*. This book will equip you with the tools needed to secure your products and your company. Whether you are a technical or a non-technical professional, this is designed to be an essential read for you.

If you want to break into cybersecurity and get a big picture of the industry, this book will help you.

Figure 5: Who is this book for?

We'll start with two questions:

1. Why is it essential for you to know about cybersecurity?
2. Why is it so important now?

As mentioned, there is an ocean of information in front of you, but what information is *relevant* to you? Furthermore, how will you put this information into context and apply it to your initiatives? Considering cybersecurity from the outset, when conceptualizing a new product or implementing organizational changes, is similar to prioritizing security before constructing a house. This proactive approach ensures that security measures are integrated into the foundation of your organization's projects and programs.

Projects and programs are designed to achieve certain business objectives and are associated with a company's business strategy. Projects are conducted to create new products, provide new services, or bring about change in the organization. Programs are a group of similar or related projects.

We will look at security, privacy, and compliance through the triple constraints that projects work within. Triple constraints are scope, time, and cost. Like the three legs of a stool, the project is crucially dependent on considering all three of these values for each task, transaction, and decision.

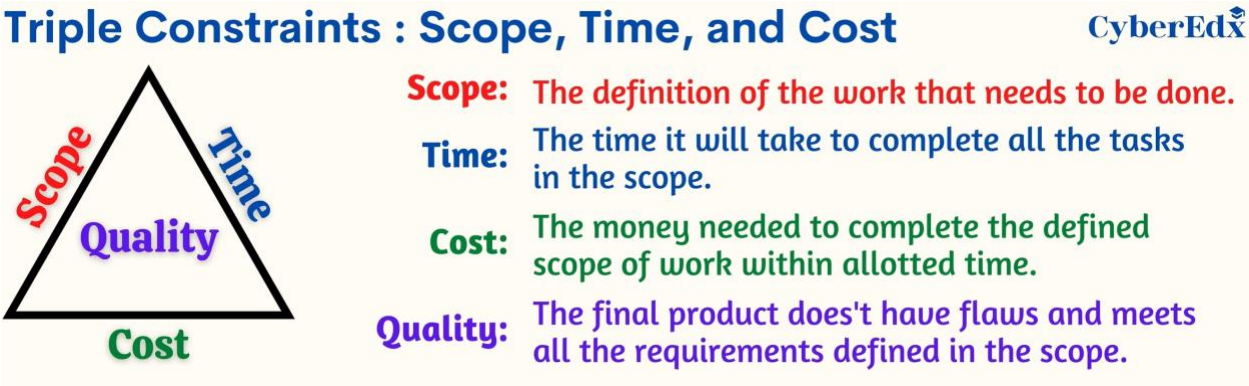

Figure 6: Projects work within the triple constraints of scope, time, and cost.

Let's review these constraints with an example.

Scope: An online shopping enterprise that has invested in a project to improve their customers' user experience during the Christmas shopping season. The enterprise has both explicit and implicit expectations about how straightforward, intuitive, and efficient the customer's user experience should be. This defines the scope of the project. The definition of the work that needs to be done is called the **scope** of the project.

Time: The enterprise would want the project to be completed well before the Christmas rush so that customers can use the improved website for their shopping. The duration required to complete the project is referred to as **time**.

Cost: Finally, the online enterprise is investing in this project by acquiring technology and software, assigning personnel, hiring third-party consultants, and contracting with service providers. All these require money. **Cost** is the money needed to complete the defined scope of work within allotted time.

The triple constraints – scope, time, and cost - have a significant impact on the quality of the products that result from your project. **Quality** is defined as the extent to which the project meets its intended purpose and satisfies customer expectations. In other words, it's about meeting the requirements and expectations of the stakeholders involved in the project. Achieving a high level of quality is essential to the success of any project, as it determines whether the project has delivered what it was supposed to, and whether it has met the needs of the people it was intended for.

Incorporating security, privacy, and compliance into your projects can significantly affect their scope, time, and cost. However, this effort is not in vain as it also has a significant positive impact on the quality of the products or services. With the integration of security measures, the products your team creates will be fortified and resilient against potential threats. Overall, although this process may require additional

resources and time, the resulting benefits to the products' robustness, security, and compliance are invaluable.

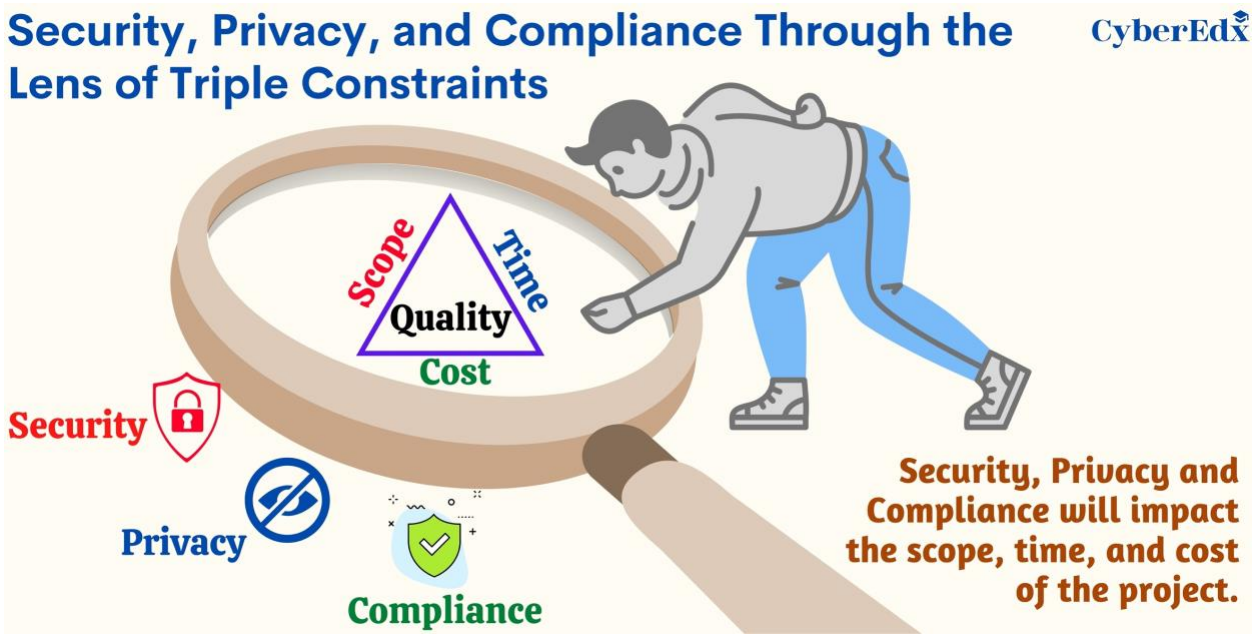

Figure 7: The scope, time, and cost will change to incorporate security

As previously stated, there is a tremendous *shortage* of qualified security professionals worldwide. That shortage may impact your organization in several different ways. And quite frankly, the longer that your projects are running without integrated security experts and resources, the more likely it is that they will release vulnerable products.

Our goal with this book is to instill a sense of urgency with respect to getting all your security "ducks in a row". It will provide you with a framework for incorporating security, privacy, and compliance into your products and services from the start. The framework will help you bake security into your products regardless of the methodologies and practices adopted by your organization and team.

The two most important project methodologies adopted by the organizations are **waterfall** (Figure 7) and **agile** (Figure 8) methodologies. The key difference between agile vs. waterfall is that waterfall breaks down software development into distinct stages that happen one after another, while agile advocates dividing the project into small iterations to deliver the product in small working parts that the users can evaluate. The demand for rapid development of new products in business has led to the adoption of agile methodologies. Agile enables teams to deliver value faster, with higher quality and predictability, and with greater adaptability to change. Delivery teams strive not only to meet due dates, but also to surpass their competitors' quality standards and release schedule.

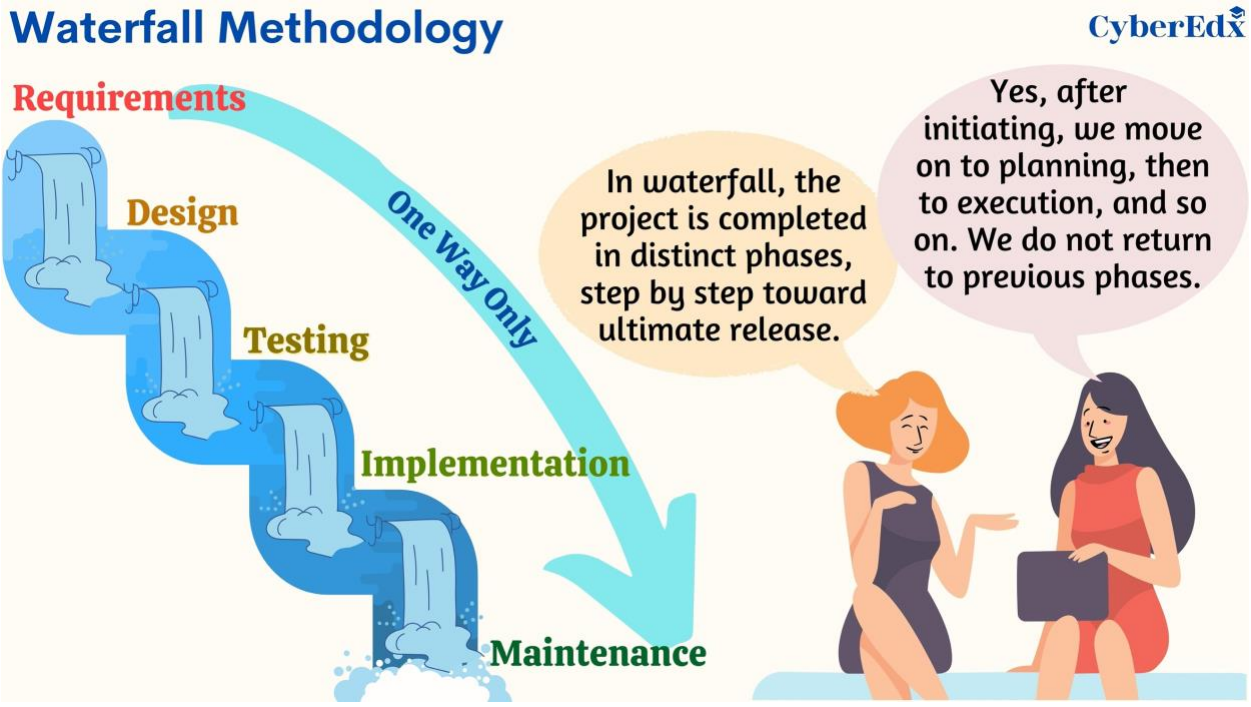

Figure 8: In waterfall methodology, the project is completed in sequential stages

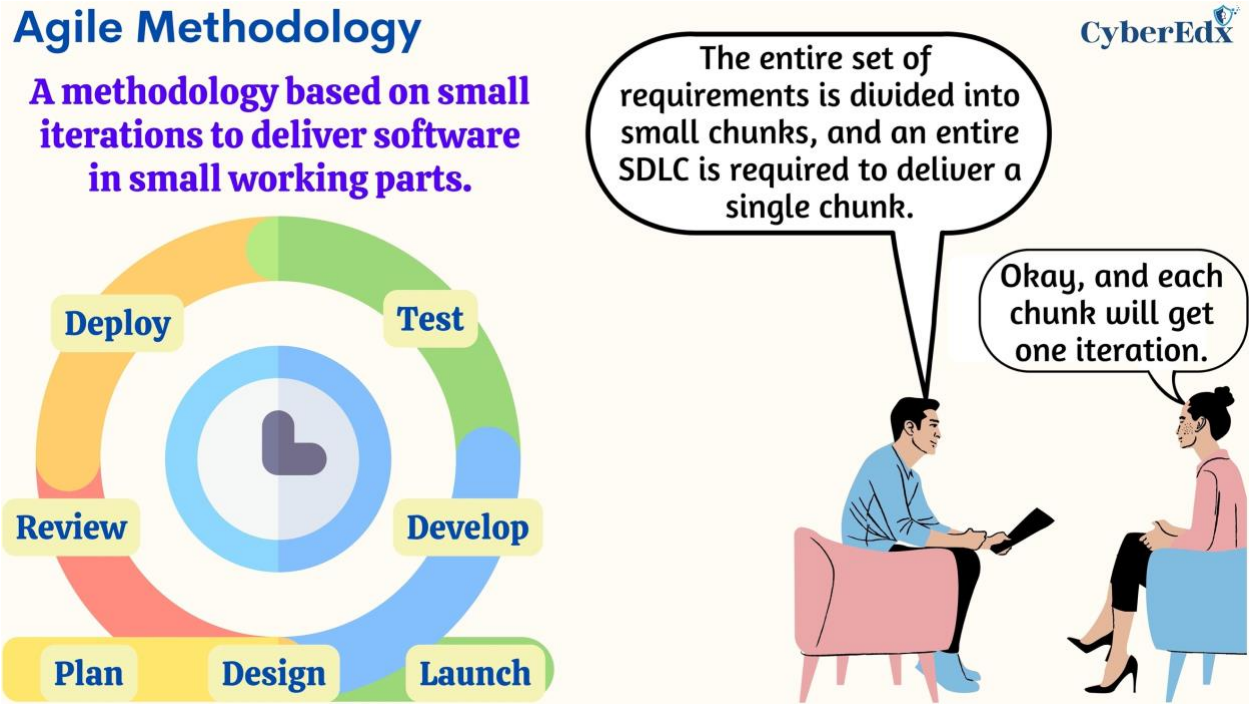

Figure 9: Agile methodology divides the project into small iterations

Another trend that businesses are adopting is **DevOps**, which involves development and operations teams working together to shorten the development lifecycle and improve quality.

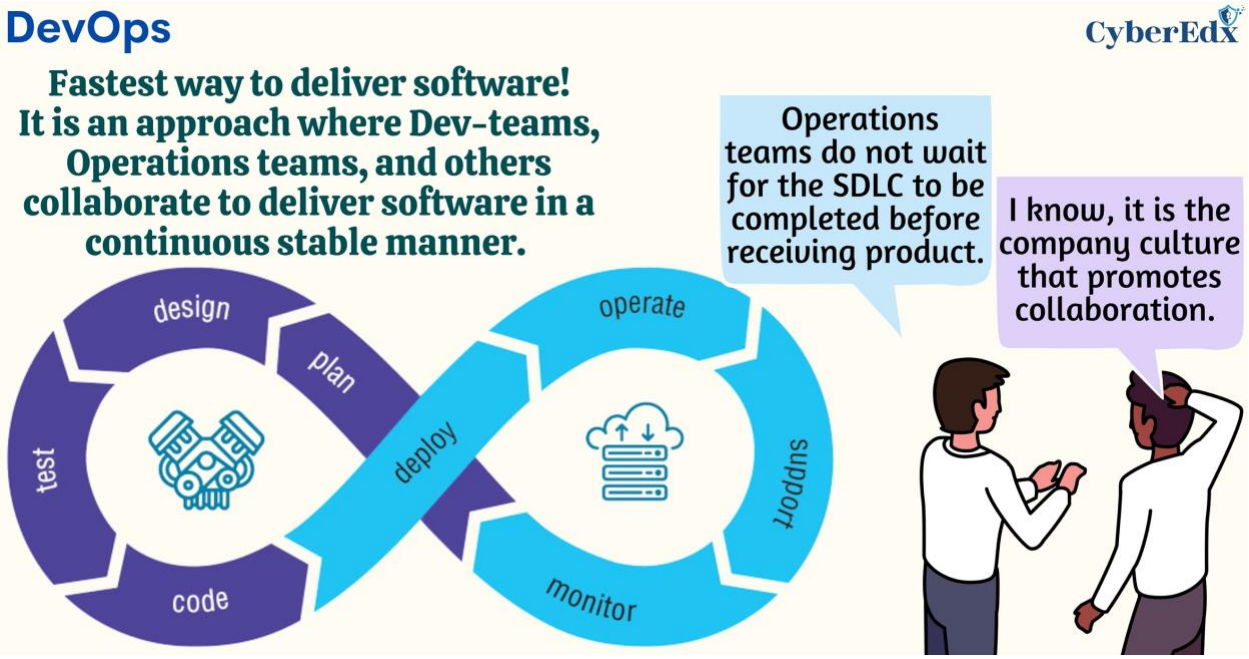

Figure 10: DevOps practices for faster delivery

Regardless of whether you operate in a waterfall or agile environment or have implemented DevOps practices, it is essential to prioritize security and compliance in your projects. This can be accomplished by considering security and compliance from the beginning of projects and ensuring collaboration with various stakeholders to prioritize it in your projects. The book is divided into four parts.

Part I: Security Foundations

- **'Chapter 1: Why Cybersecurity?'** defines security and privacy, and why they are critical in today's digital age.
- **'Chapter 2: Basic Terms'** discusses the key cybersecurity concepts and definitions that you should know.

Part II: Risks and Compliance Frameworks

- **'Chapter 3: Risks'** discusses the risks you should be aware of. We have divided the risks into two categories: project risks and enterprise risks.
- **'Chapter 4: Compliance Frameworks'** explores the compliance frameworks and standards that you should follow to ensure that your projects are compliant with regulatory requirements.

Part III: Practical Application

- **'Chapter 5: Start on the Right Foot'** discusses the actionable steps you and your team must take to create secure and compliant products from the beginning.

- **'Chapter 6: Plan for Success'** explores how to embed security into your projects and release plans and provide practical guidance on identifying and managing security risks.
- **'Chapter 7: Execute for Excellence'** covers building or enhancing products with a security mindset. This chapter goes over secure software development lifecycle in detail.
- **'Chapter 8: Keep a Close Watch'** provides specific guidance on monitoring the project activities from a security and compliance perspective. We'll also introduce you to various tools.
- '**Chapter 9: Conclude on a High Note'** discusses the security and compliance activities in the closing phase of the projects.

Part IV: Action Plan

- **'Chapter 10: Being Cybersmart'** discusses developing an action plan for your projects and attributes of a cybersmart professional.

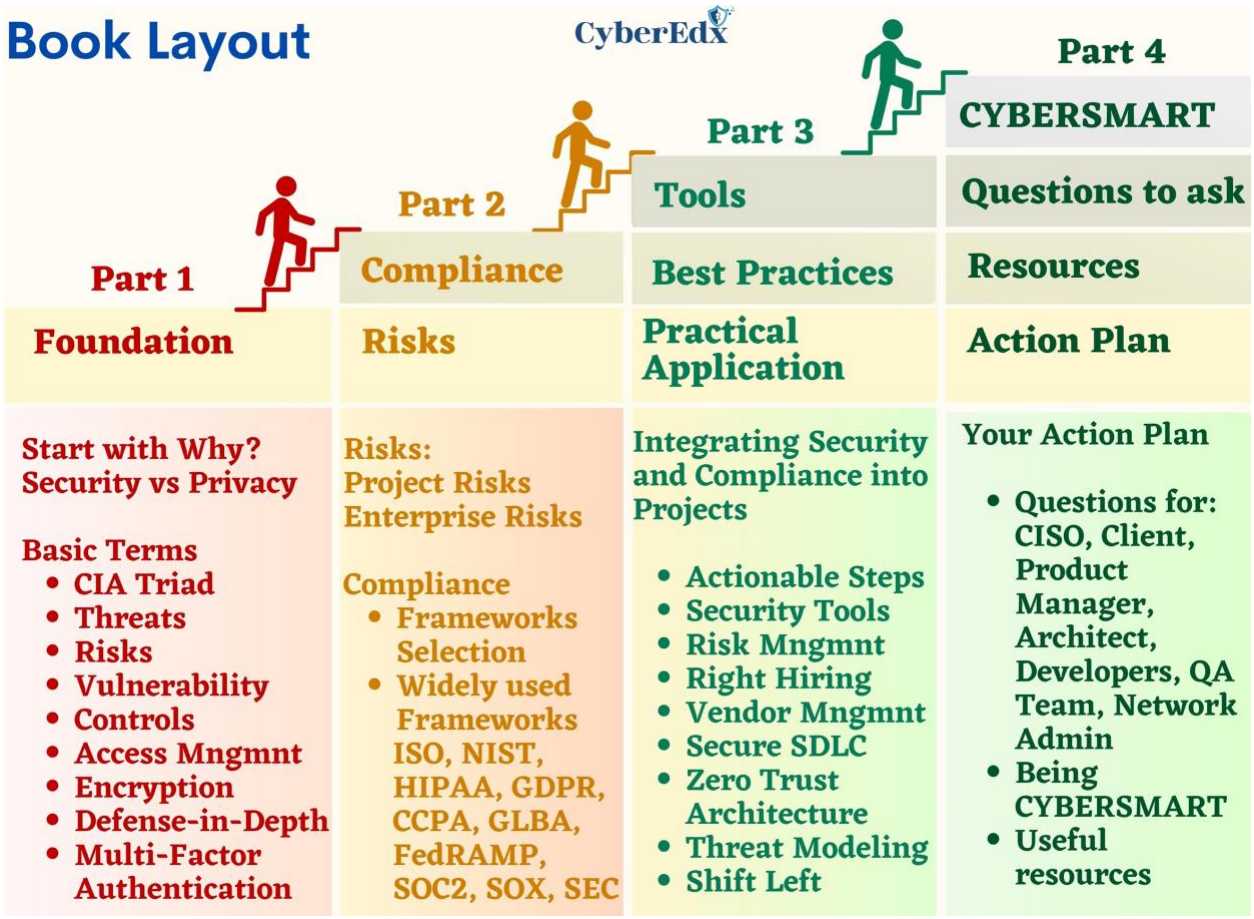

Figure 11: Your journey from the foundation to becoming cybersmart

Part I
Foundations of Cybersecurity

CHAPTER 1

Why Cybersecurity?

Figure 1.1: Integrating security and compliance into projects

Assume you are a project leader under intense pressure to deliver projects that will meet the deadline, stay within budget, and maintain high-quality standards. In addition, you are now responsible for incorporating security and compliance into your projects and products which may sound daunting. However, understanding the foundations of cybersecurity and the trends driving security demand will assist you in driving this effort.

In this chapter, we will cover the foundations of cybersecurity. When we use the term cybersecurity, we mean the security and privacy of digital assets. Let's dive into these terms in detail.

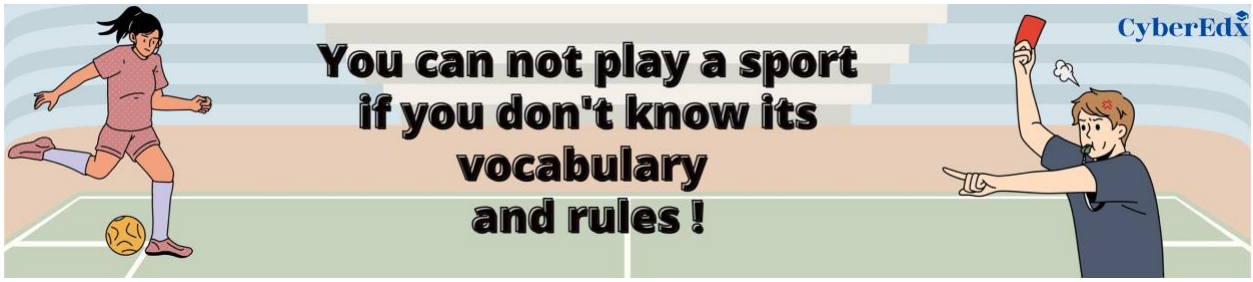

Figure 1.2: It all starts with vocabulary

Security

In simple terms, *security* means the measures taken to be safe or protected. In our daily lives, we do a variety of things to keep ourselves safe and protected. For example: when we leave the house, we lock our doors. We do that to safeguard our critical assets which include electronic devices, gadgets, and critical documents.

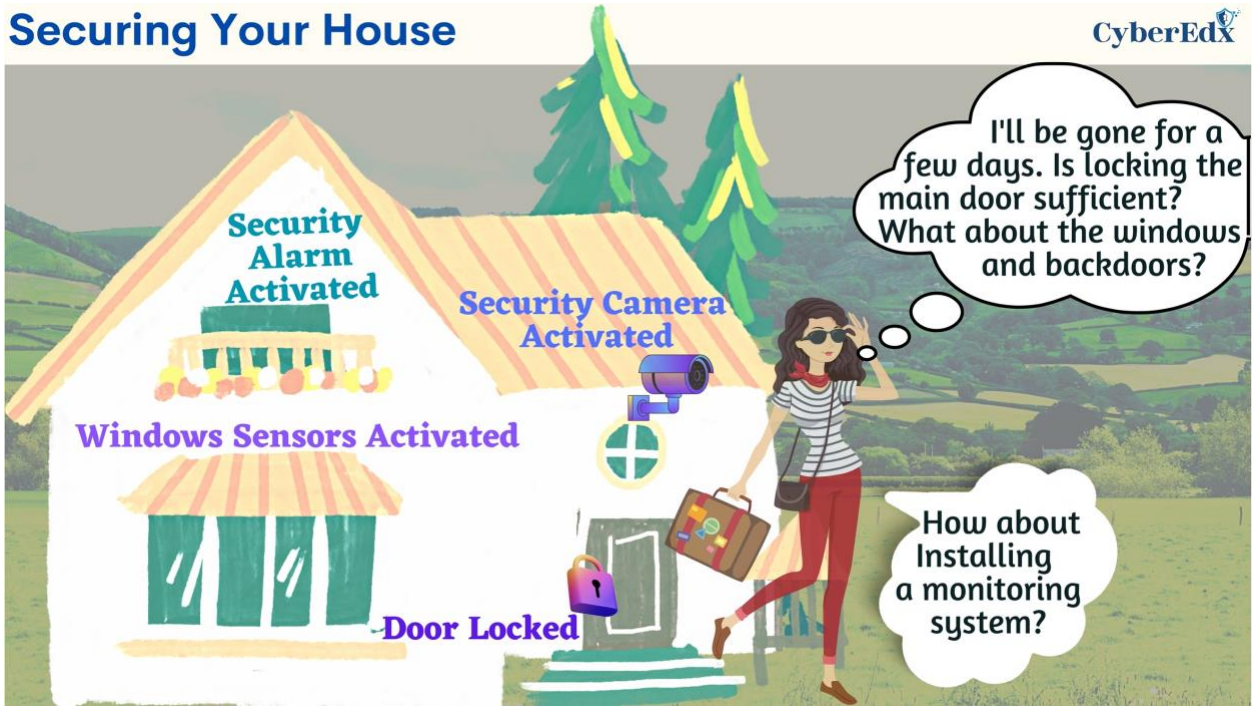

Figure 1.3: We use a variety of methods to secure the house

In this case, the lock is only *one* layer of security. But why is it just one layer?

Locking the door simply isn't enough to prevent theft. What about the windows and the back doors? They, too, must be closed properly, locked, and secured. Devices like monitoring cameras, alarm systems, sensors, and others serve as additional layers in preventing theft. In a nutshell, when we take these preventative measures, we are securing the assets and information in our house and, hence, implementing security.

Similarly, your project will utilize various physical resources, i.e., work-computers, servers, network appliances, server rooms, critical documents, etc. Your projects may use some software tools and may create software resources i.e., applications, and programs. These software applications will exchange sensitive information over the company intranet and the internet, which is accessible to your end users and cybercriminals from anywhere in the world.

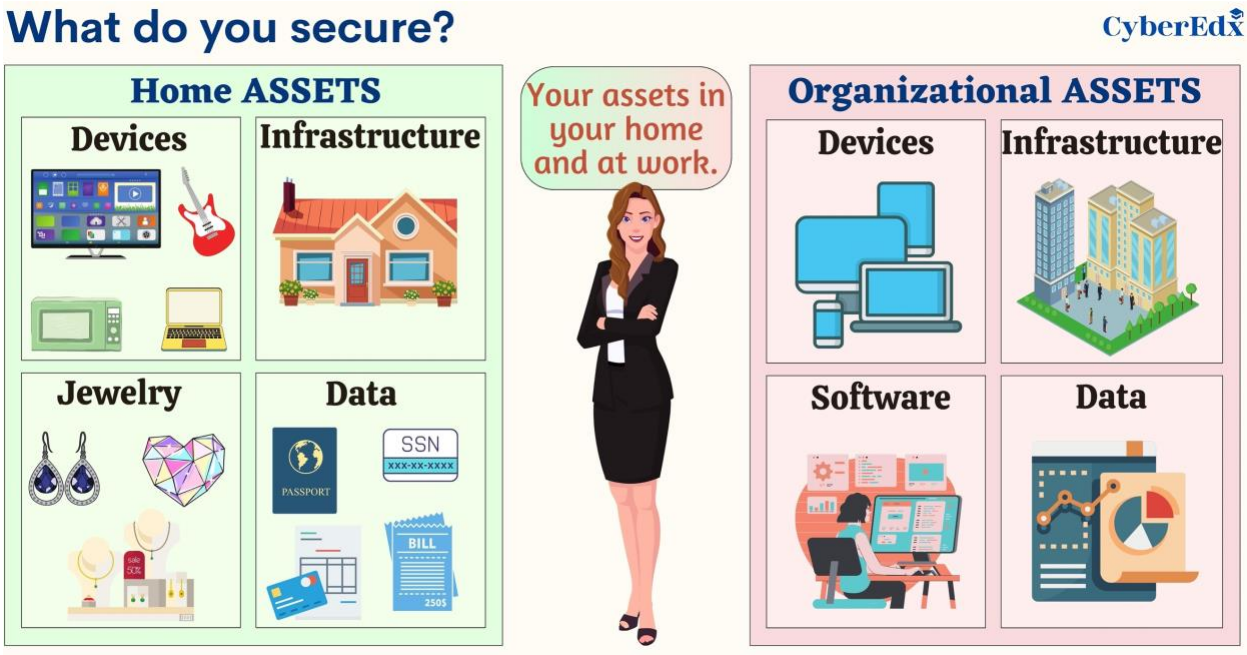

Figure 1.4: Examples of assets that must be protected

How do you protect your company's assets and information? You put in technologies, processes, and policies, as well as engage professionals, to protect your company's sensitive data and other assets.

Therefore, **security** is defined as implementing technologies, processes, and practices to protect your assets and information from unauthorized access and use.
You must be aware of these technologies, processes, and practices to protect the assets and information.

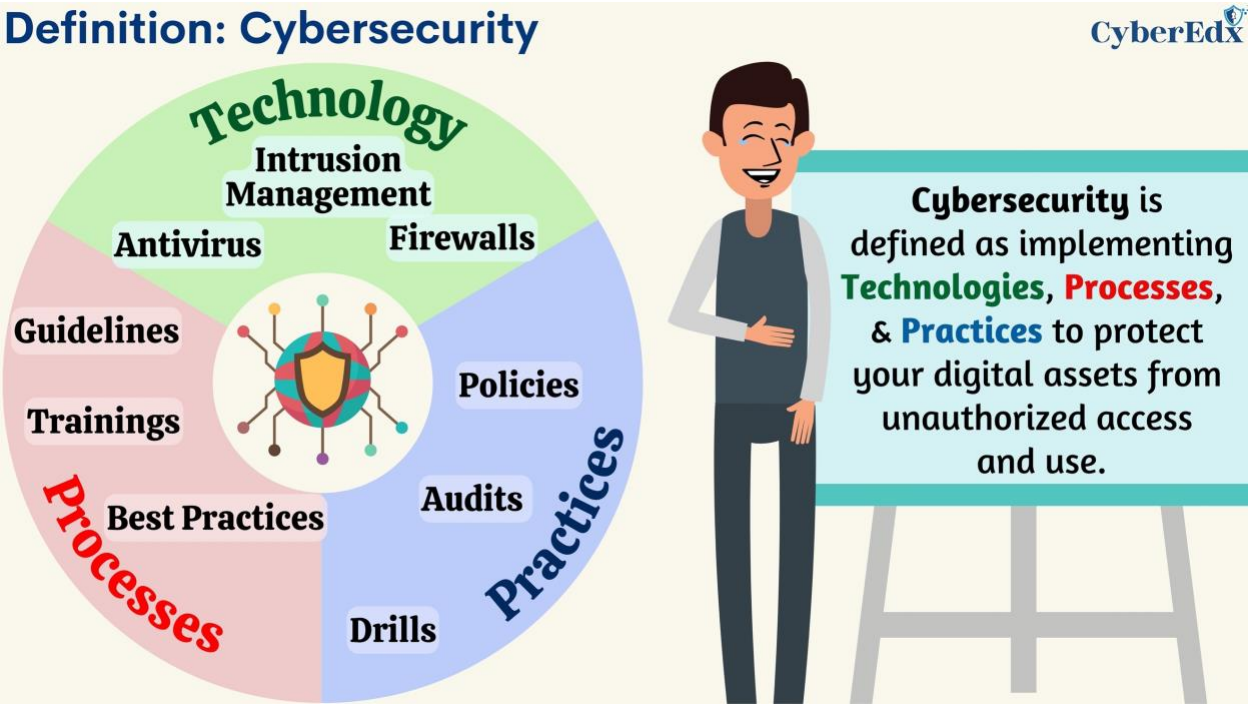

Figure 1.5: The definition of security

Privacy

Privacy is keeping your personal, critical information to yourself or to the people you earnestly trust.

When we host parties, we welcome guests into our home. We give them access to the living hall, kitchen, restrooms, and other common areas. However, do we allow them any access to sensitive information such as your social-security-number (SSN), mother's maiden name, credit card, and bank account information? No. This information is our private information. This information belongs to only us and must be protected at all costs.

Let’s talk about social media. You may share your life events, pictures, and videos with friends on Facebook, Instagram, Twitter, etc. However, do you disclose your private, sensitive information in your social media posts? We're sure you don't, and you certainly would not want social media sites to do so without your consent, either. In fact, you would not want any business you deal with, whether it's your bank, doctor's office, or mortgage company, to disclose your private information without your permission.

Everyone should be able to share information while maintaining their privacy. It is your fundamental right to control how your personal information is collected and used by the businesses.

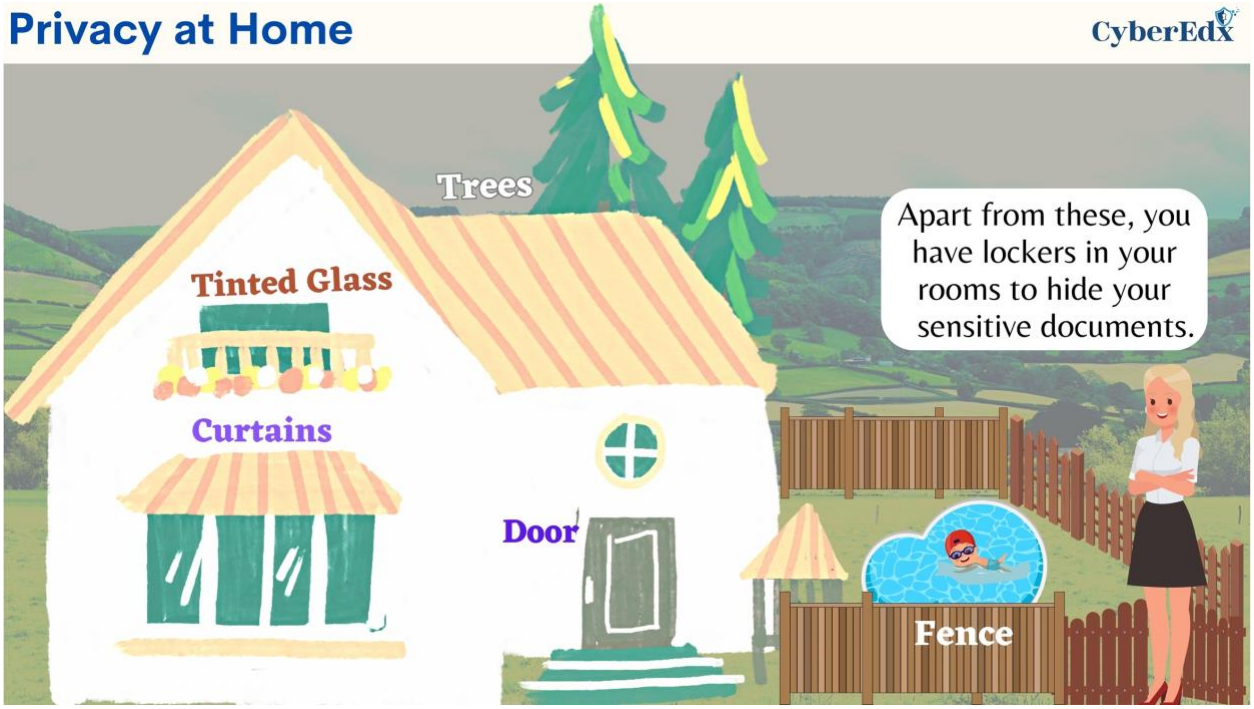

Figure 1.6: Privacy in your house

Privacy is defined as safeguarding your personal, sensitive information from unauthorized access and sharing it only with the people you earnestly trust.

Finally, let's look at privacy from a corporate perspective. Information like customer data, competitive information, and intellectual property is confidential and must not be shared with outsiders. This information needs to be protected. There must be appropriate safeguards in place to protect this data.

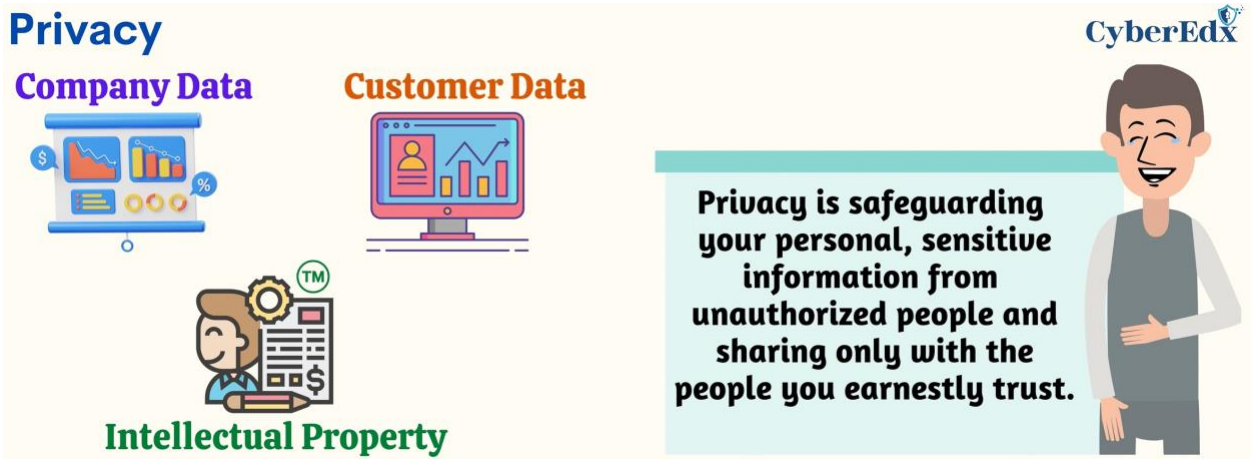

Figure 1.7: Privacy definition

Depending on the industry you are in or the type of data your projects are handling, government regulations play an important part in defining privacy. We will cover these regulations in the following chapters.

You must ensure that your projects and products don't create a flaw or weakness that exposes confidential and sensitive data to unauthorized people.

Often people use the terms 'security' and 'privacy' interchangeably. Let's understand the distinction between security and privacy with the following example.

Lily and Mary live in the same house but in different rooms. They both want to protect their house from the robbers. They have doors, locks, security cameras, sensors etc. in place for security. But they value their privacy and don't want to share their sensitive information with each other such as SSN or who they are dating.

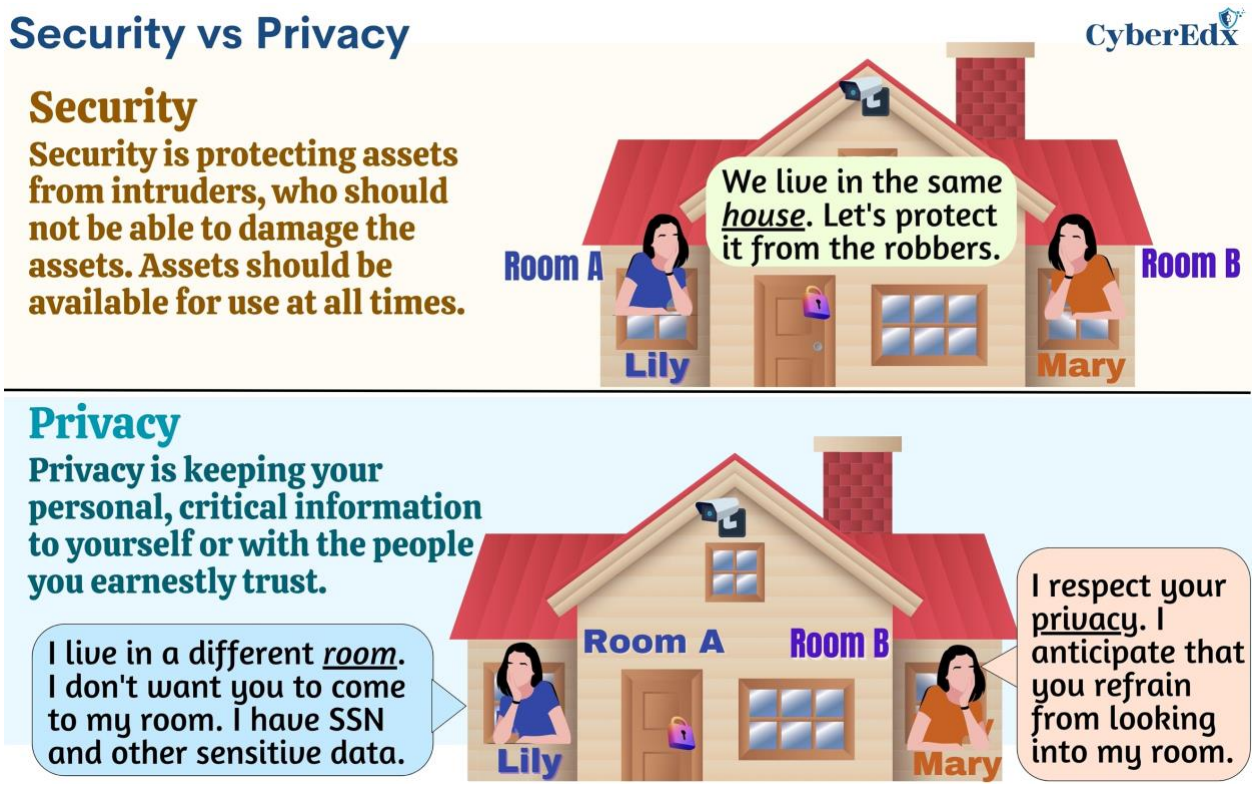

Figure 1.8: Difference between security and privacy

Exercise 1.1:

Identify the critical personal information you will be collecting from your customers.

Start with Why

What is driving the demand for security and privacy in products and services? Here are some of the key factors to consider:

1. Digitalization
2. Increase in Attacks
3. Compliance

Figure 1.9: Trends driving the demand for security

Let's go through each of these in depth. To make it easier and to remember, we'll refer to these as **DAC**.

Digitalization

Digitalization is the process of converting paper information into a digital format so that it can be used by computers. We have seen massive digitalization in this past decade. Our information, which was previously stored in cabinet files, notebooks, and so on, is now available in digital format where we can instantly access it from all our devices from anywhere in the world.

People use their phones and laptops to do things like banking, grocery, shopping, and more. The amount of time spent on electronic devices has risen dramatically in recent years, as work and social lives increasingly move online.

Customers who used to interact with companies physically or through phone calls now use digital devices and social media to communicate. Organizations are rapidly

adopting technologies to automate their processes and provide a better user experience to their customers. For example, banks and retailers have websites and mobile apps that allow customers to bank and shop without leaving their homes. COVID-19 further accelerated the deployment of digital technology.

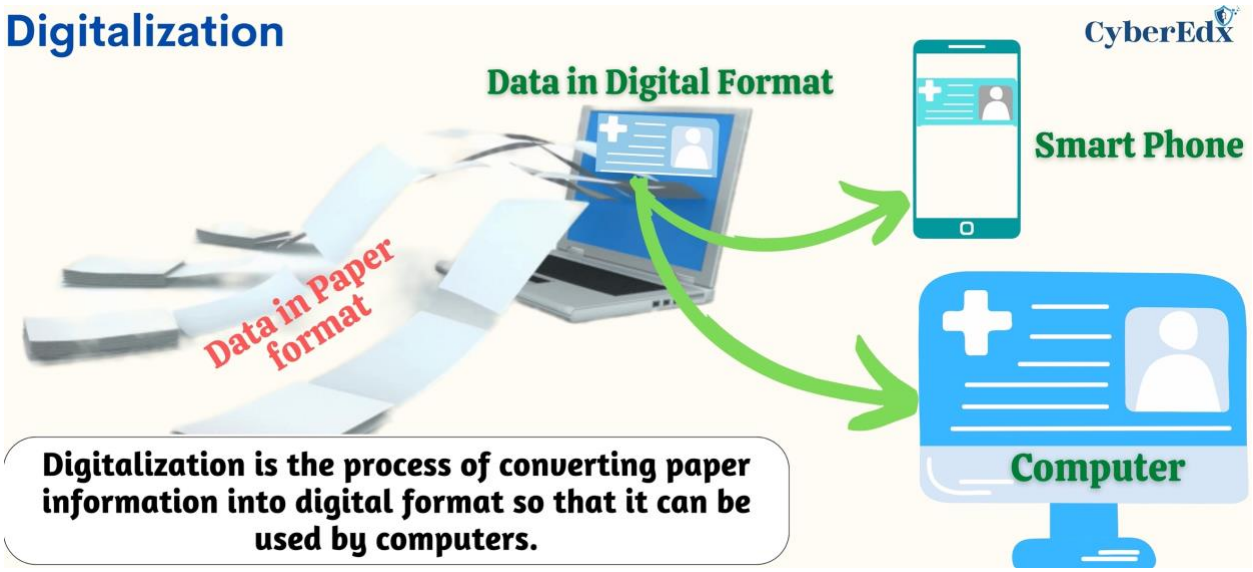

Figure 1.10: Digitalization defined

Digitalization is more than just converting paper documents to digital formats. Our household items are now digital as well, which means they are linked to the internet. We can now control these devices remotely now that they are online.

There are connected devices all around us—phones, vehicles, and household items like coffee makers, refrigerators, microwaves, etc. These connected devices are often referred to as **IoT**—the Internet of Things.

With the introduction of 5G, our devices are more connected than ever before. 5G is the fifth generation of cellular networks. Up to 100 times faster than 4G, 5G is creating never-before-seen opportunities for people and businesses.[7]

Statista, a market, and consumer data company, predicts that the number of IoT-connected devices worldwide will reach 38.6 billion by 2025.[8] Additionally, forecasts suggest that by 2030 around 50 billions of these IoT devices will be in use worldwide, creating a massive web of interconnected devices spanning everything from smartphones to kitchen appliances.

[7] https://www.ericsson.com/en/5g

[8] https://www.statista.com/topics/2637/internet-of-things

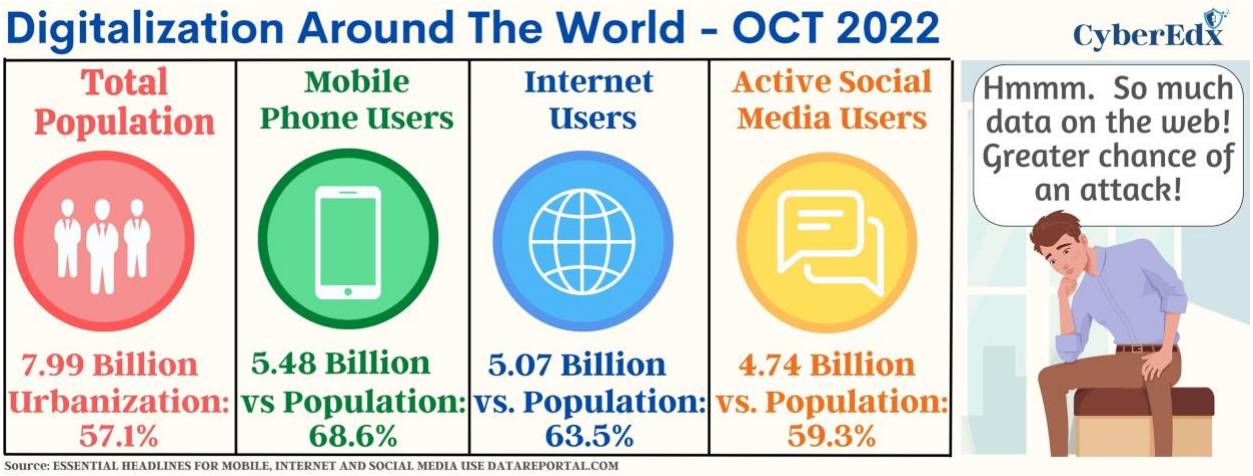

Figure 1.11: Data about the world's mobile phone, internet, and social media users

Source: www.datareportal.com

So, digitalization is happening at a rapid pace. But why should you be concerned? Rapid digitalization has raised cyber threats. Any device connected to the internet can expose vulnerabilities.

At your work, your products may collect and generate a large volume of data that must be protected. As part of digitalization, sensitive data travels through the internet. There may be hackers sitting in between, say, your company and your customer's mobile phone, to intercept it. If they get this information, it may be misused.

Furthermore, your organization may store data in the cloud. The "cloud" refers to hardware, software, and services that run on the internet, instead of locally on your company servers.

Cloud computing's rapid adoption has changed the way businesses store, process, and access data and applications. When compared to traditional on-premise infrastructure, cloud computing provides numerous advantages, including increased scalability, flexibility, and cost savings. According to Gartner, over 95% of businesses will use cloud computing by 2025. [9]

You must know what data is being kept in the cloud and how it's being secured. Your organization's applications may run on mobile and IoT devices, and it's essential that the applications, devices, and information be protected.

You and your team must be aware of the new risks associated with digitalization and be prepared to deal with them.

[9] https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences

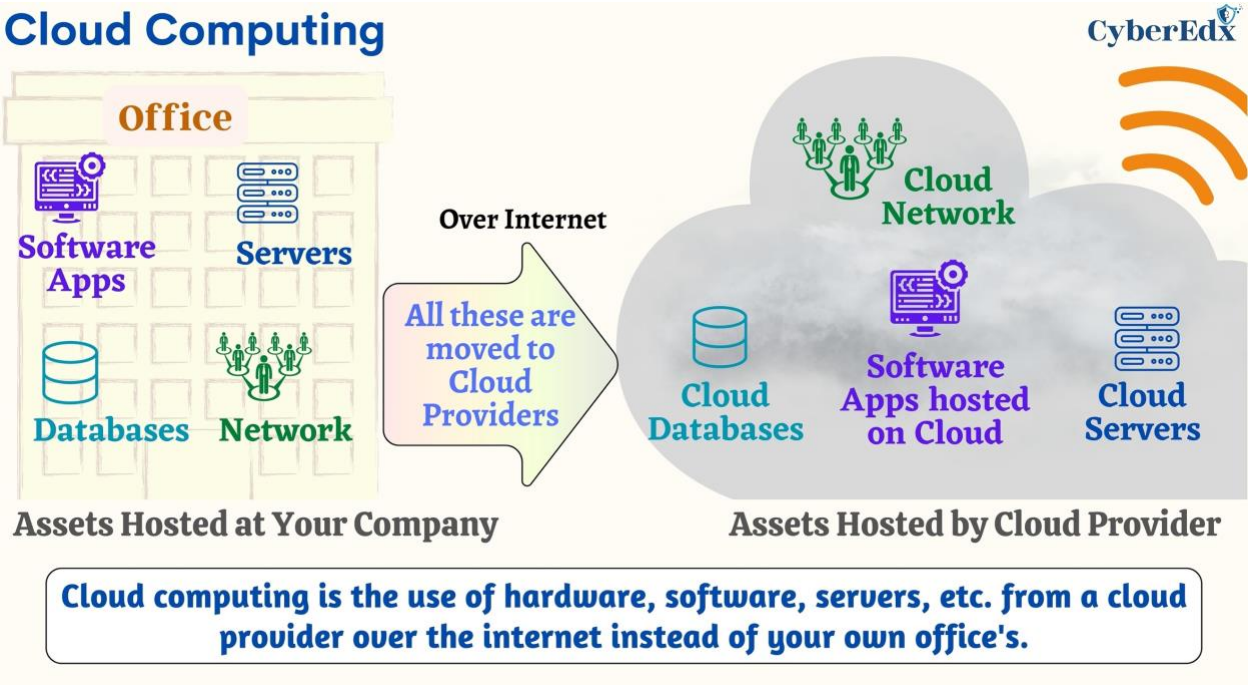

Figure 1.12: Cloud computing explained

Increase in Attacks

The growing frequency and severity of cyberattacks on vital infrastructure is widely regarded as one of the most serious problems of the current decade. Recent cyber-attacks support this assertion. The breach into *SolarWinds*, which is thought to have been coordinated by Russia's intelligence agency, and the hacking attack on critical systems, which was most likely carried out from China, revealed the growing number of attackers worldwide and the sophistication of the tools they have been using. In Russia's war on Ukraine, various destructive cyberattacks were launched against the government and critical infrastructure in Ukraine.

Another factor that contributed to the increase in attacks was the COVID-19 pandemic which dramatically changed how the world does business. Almost overnight, nearly all government and private firms were relocated from an office building to a work-from-home environment. You and your team members may have also started working remotely during the pandemic and may still be remote.

In a home office, the risk of cybercrime is very high. Internet connections are not as secure as in the office. Confidential information may be intercepted in virtual meetings, which is unlikely in the in-person meetings held in closed rooms.

This crisis has been a perfect storm of security disruptions. We've seen an increase in threats because organizations were increasingly fragile during this time. Many

employees and customers have been quickly exposed to new technologies, applications, and processes with which they were not previously acquainted. Employees, for example, had to learn video conferencing and other collaboration tools in order to stay connected and effective while working remotely.

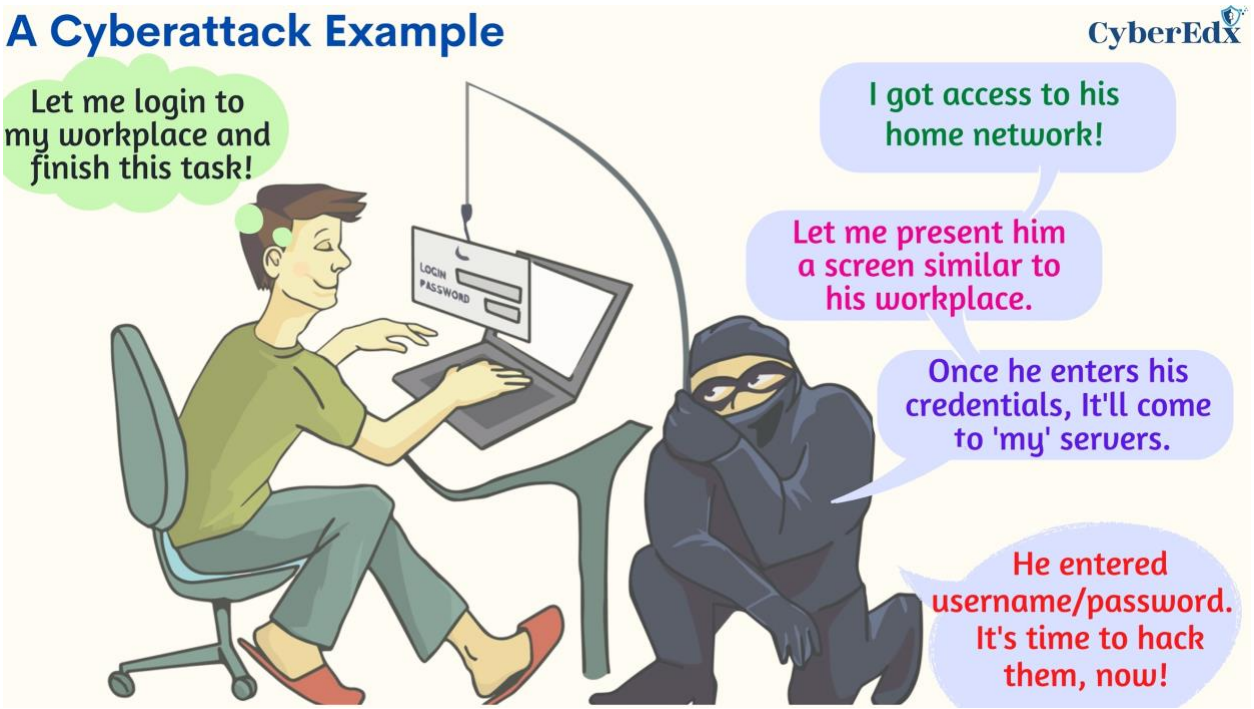

Figure 1.13: Hackers trying to steal your personal information

According to the *PurpleSec* 2021 report, there was a 600% increase in cybercrime due to the COVID-19 pandemic.[10] During the pandemic lockdown, cybercriminals were also working from home. They got an opportunity to hone their skills to be more efficient at cyberattacks. Sometimes the attackers have financial motives. Sometimes, they want to disrupt the operations of a company.

The dark web* provides access to countless breach and attack techniques for anyone interested in expanding their repertoire. The dark web is made up of websites that cannot be discovered by search engines and are not available to everyone. Special browsers are needed to access the dark web.

[10] https://purplesec.us/resources/cyber-security-statistics/

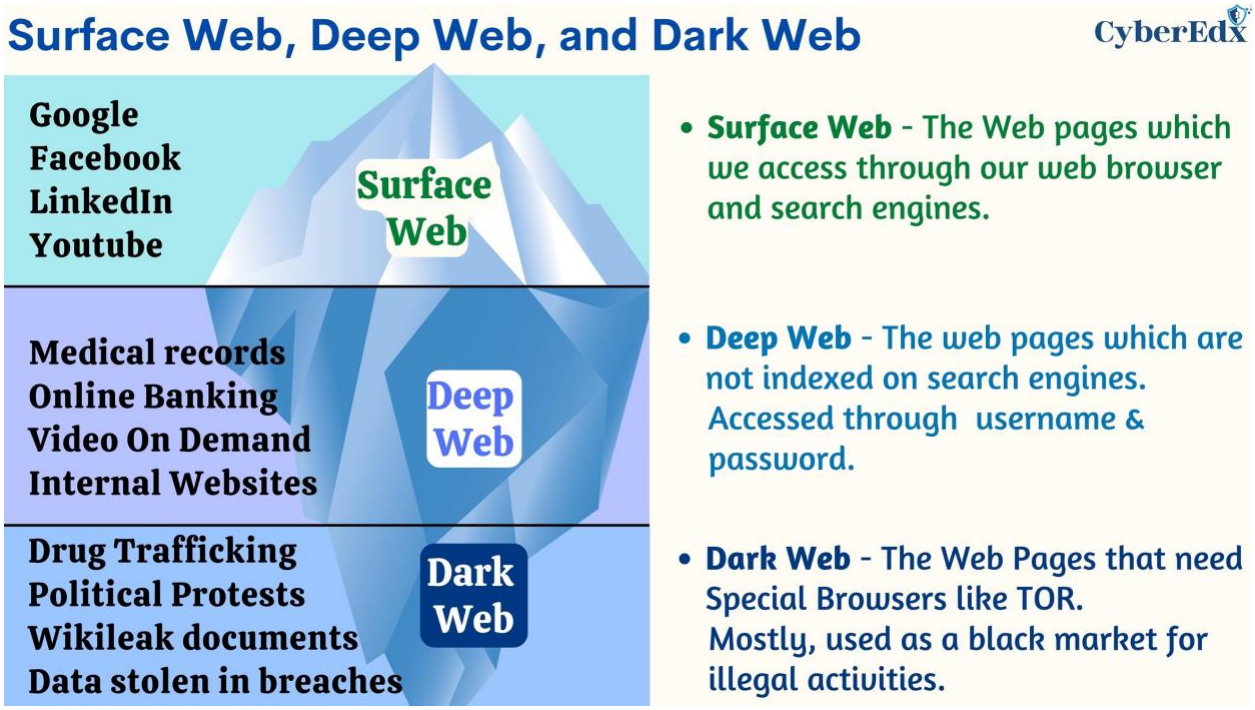

Figure 1.14: Web, deep web, and dark web explained

Cybercriminals recognize that businesses are struggling to keep up with technological developments and protect their data at the same time. Since the development team is constantly on the go to build new products and features, they sometimes forget to prioritize or even include security. Frequently, they ignore it, expecting the security team to look after the issue.

This gives well-prepared, skilled cybercriminals the ability to easily pounce on any opportunity. That's the reason the number of organizations victimized by cybercrime is growing significantly.

Figure 1.15 shows the percentage of organizations compromised by at least one successful attack over the years as per a report done by *CyberEdge* group by interviewing 1200 IT security professionals in 17 countries and 19 industries.

You and your teams must be well-informed about recent attacks and the vulnerabilities that were exploited by the attackers. It's advisable to discuss recent attacks and breaches, as well as the vulnerabilities that caused the attacks in the team meetings. This knowledge will help your team watch out for similar vulnerabilities in your applications.

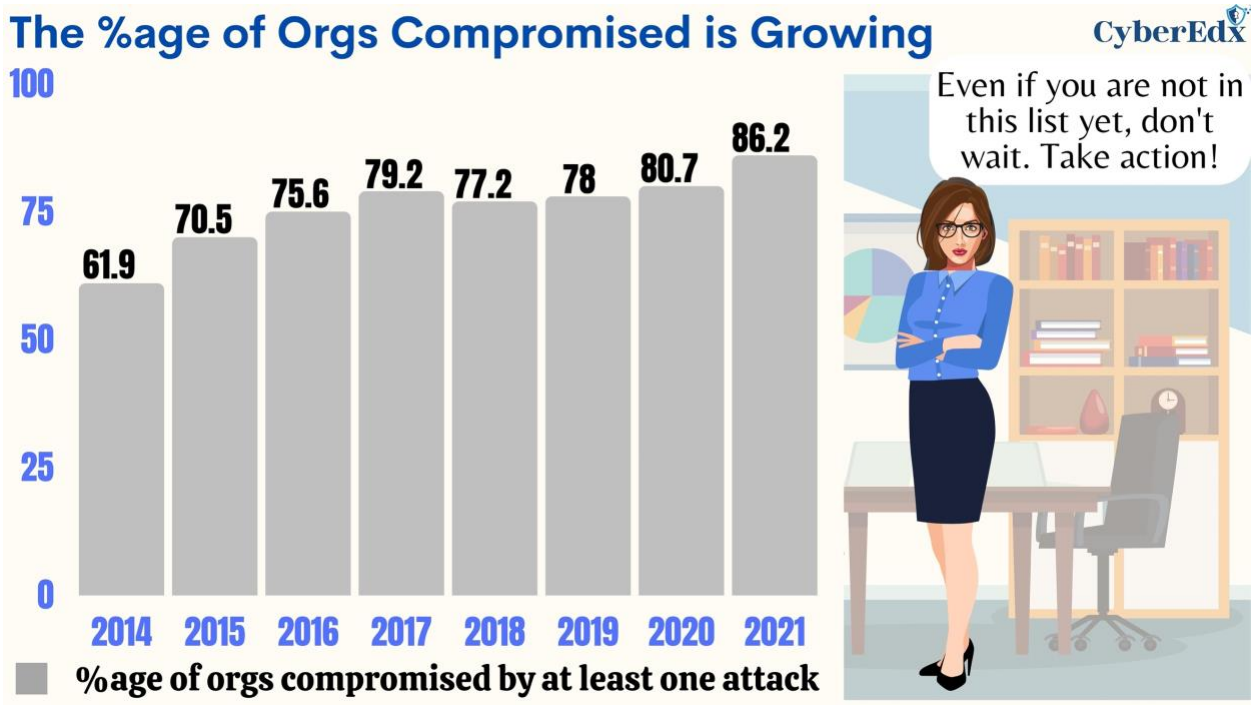

Figure 1.15: Percentage of organizations compromised by attacks *Source: CyberEdge*

Laws and Regulations

The number of laws and regulations that require businesses to adhere to legal, security, and privacy standards is growing. The project teams are expected to collaborate with security and legal experts to determine which regulations apply to their projects and to ensure that they are followed.

What laws and regulations should your product comply with? This depends on the industry, type of business, services provided, and some standards that your local government requires. For example,

- Any company that accepts credit card payments must adhere to the **PCI-DSS** (Payment Card Industry-Data Security Standard)
- Healthcare organizations must comply with **HIPAA** (Health Insurance Portability and Accountability Act) to protect patients' sensitive data.
- **SOX** (Sarbanes-Oxley) affects all publicly traded firms in the United States.
- **ITA** (Information Technology Act) is India's law highlighting the punishments and penalties safeguarding e-banking, e-commerce, and e-governance sectors.

- **GDPR** (Global Data Protection Regulation) is a law created in the European Union (EU) to protect the personal data of its citizens. Any company that deals with the data of EU citizens must abide by this law.
- **APP** (Australian Privacy Principles) is Australia's data privacy and protection regulations for the collection use and disclosure of personal information.

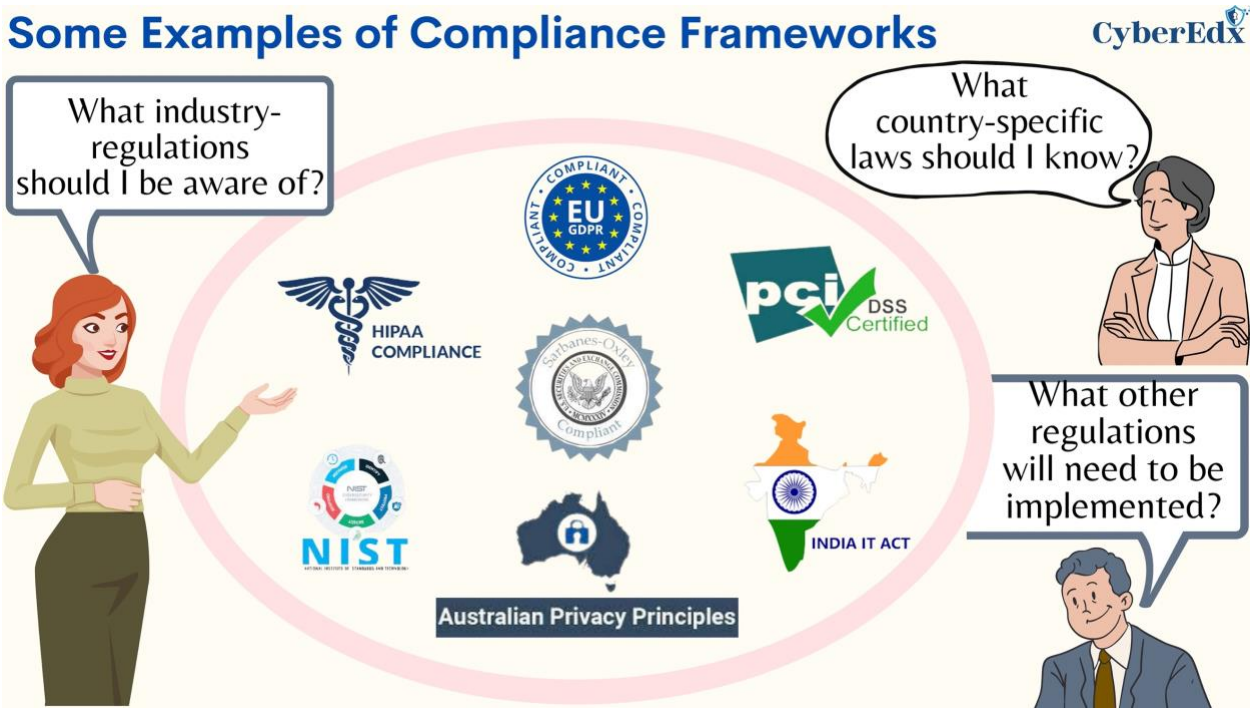

Figure 1.16: Questions regarding regulations you may have

In addition to compliance regulations, some businesses must obtain certifications such as ISO 27001 to demonstrate that they have security processes and controls in place to protect their customers' data. Another type of certification is HITRUST, which is required by some healthcare organizations in the USA.

SaaS (Software as a Service) companies may be required to undergo SOC1/SOC2 (Service Organization Control) audits to demonstrate to their prospective clients that they have processes in place to keep their data safe. Clients may request certifications and audit reports from vendor companies before entering into a relationship with them.

You may believe that you already have too much on your plate, and now you have to comply with regulations or work toward certifications and audits. Complying with these regulations may be perceived as a burden by your team members. However, these frameworks have simplified the process and provided the baseline requirements when it comes to cybersecurity. Since these rules enforce some basic cybersecurity standards,

we don't have to start from scratch. These frameworks have rules and guidelines for your teams to follow.

It is critical for you to be aware of the latest compliance, certification, and audit requirements for your products. You may need to factor in the time and budget for the security team to analyze and provide feedback. You should also account for the time it would take to fix any issues that the security team finds.

Summary

It's important that your products you create and services you deliver are secure. This can only be achieved when security is deeply ingrained into your processes.

Security is about preventing unauthorized access to assets such as various physical belongings, critical documents, and sensitive information. It is important for you to take measures to ensure security of your current and future assets.

Privacy refers to ensuring that sensitive information is confidential and must be kept secure from unauthorized users. You must ensure that your products do not introduce flaws or weaknesses that expose confidential or sensitive data.

The trends that are driving the demand for cybersecurity across the globe are:

Rapid Digitalization

In the last few years, there has been a massive digitalization. Digitalization is the process of converting paper information into a digital format so that it can be used by computers. To remain competitive, businesses are rapidly implementing new technologies. Your products or services may generate massive amounts of data that may be stored on the cloud, and your applications may run on the web, mobile, or IoT devices.

Increase in Cybersecurity Attacks

In the last few years, there has been a significant increase in cyberattacks. Because of the pandemic, employees were forced to work from home. This gave attackers several opportunities to target remote employees. Sometimes the attackers have financial motives. Sometimes, they want to disrupt the operations of a company. Regardless of their motives, you must be well-informed about recent attacks to ensure your applications do not introduce any vulnerabilities for the attackers to exploit.

Laws and Regulations

There are numerous general, industry-specific, and country-specific laws and regulations that your organization must follow. It is critical that you are aware of the compliance requirements. You may need to budget for the time and money it will take

for a compliance team to review and provide feedback on your in-development products.

CHAPTER 2

Basic Terms

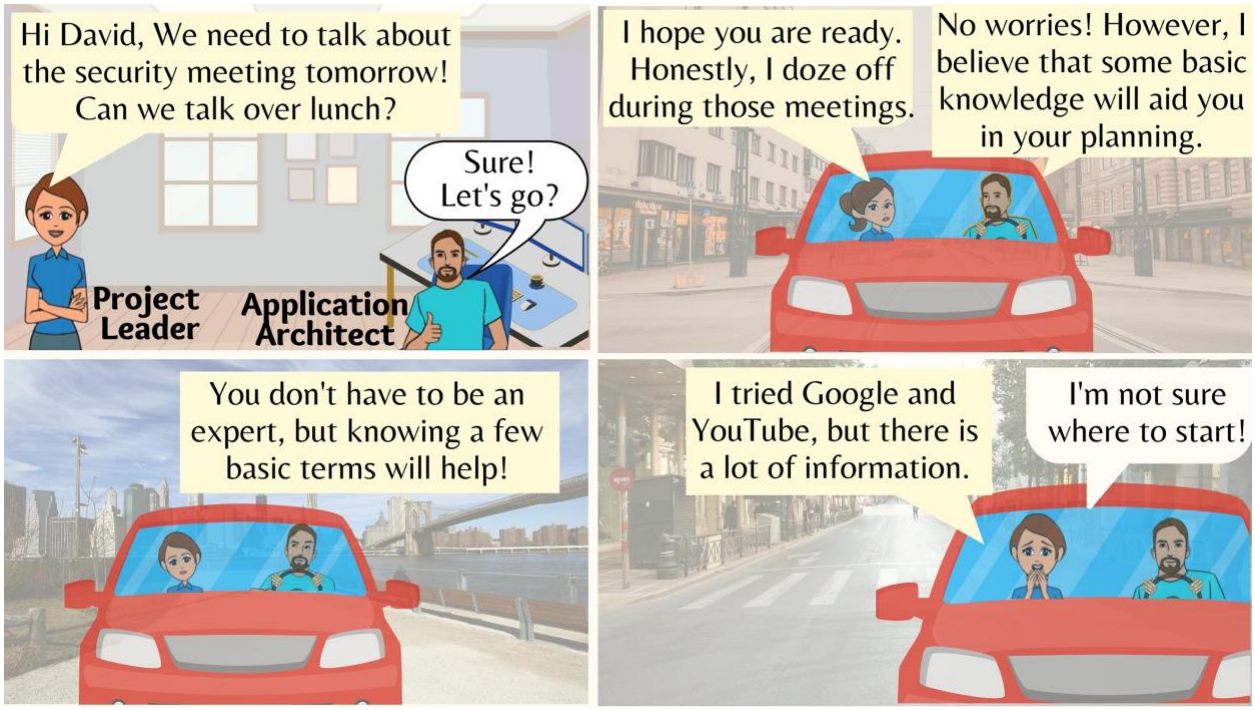

Figure 2.1: The significance of cybersecurity vocabulary for leaders

Knowledge of the basics of cybersecurity is essential for you and your team. With the wide spectrum of cybersecurity solutions and defenses at your disposal, what should be your focus? What do you need to master in order to have informed discussions with your company's security professionals? Most importantly, how do you discuss security, privacy, and compliance with your team members?

Do you happen to recall any meetings where your team was discussing security? They may have used technical jargon that you simply couldn't understand. To make yourself feel better, you might have discreetly affirmed to yourself, "Don't worry, I don't need to

know this stuff". Or you could be worried about how your team will protect the organization if they don't comprehend the jargon.

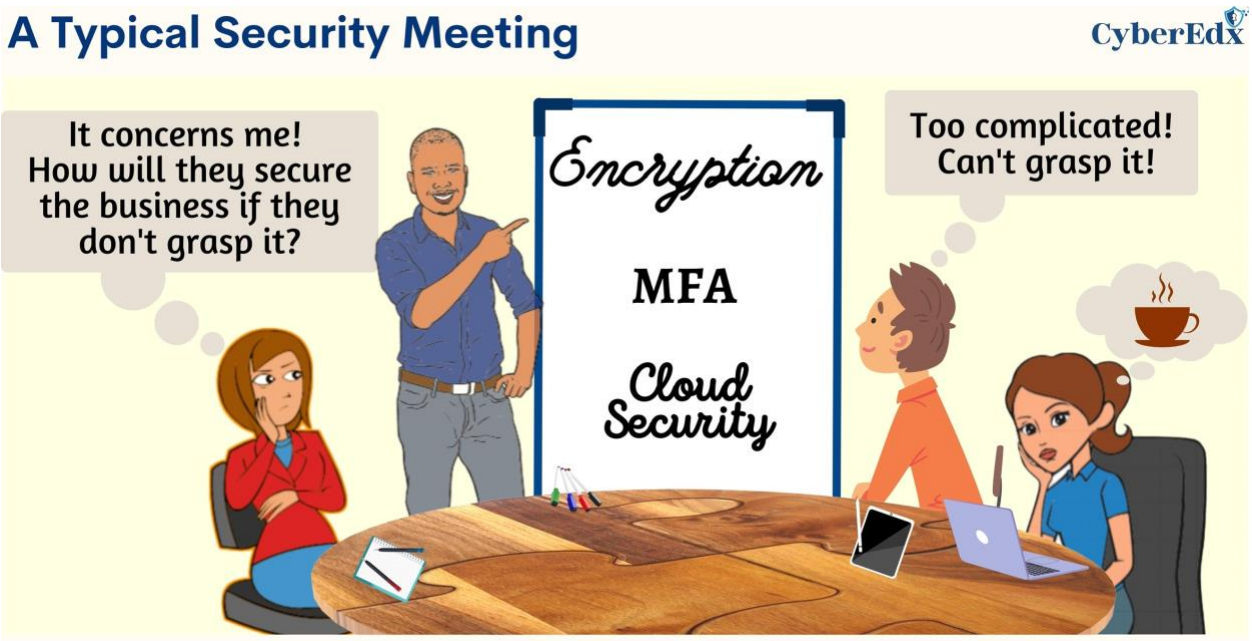

Figure 2.2: Team members discussing security in a meeting

This chapter will help you to be much more informed and knowledgeable in the event of another meeting where security is discussed. We hope that you become more vocal, utilizing the terminology you learn. Most importantly, though, you will be equipped to play a critical role in integrating security into your products and applications.

Now, let's dive into some fundamental terminology and concepts.

It's easier to understand new terms and concepts when they are contextualized. For context, we'll refer to a case study.

Case Study

Assume you work for a healthcare company, and you have been assigned as the project leader for a new project. The goal of this project is to help patients recover after hospitalization. When patients are discharged from the hospital, there is no way for doctors to monitor whether patients are really following the guidelines required for recovery.

Your team is in charge of addressing this issue by creating self-service applications that allow patients to interact with their care team and track their medication regimen, vitals, and physical activities using IoT devices. In addition, the apps will remind

patients to take their medications and schedule follow-up appointments with the care team. We chose the healthcare case study because it is something that most of us can relate to.

Because a patient's life may be dependent on your product, it is critical that patient data is not misused, medication dose data is not tampered with, and the app is always functional.

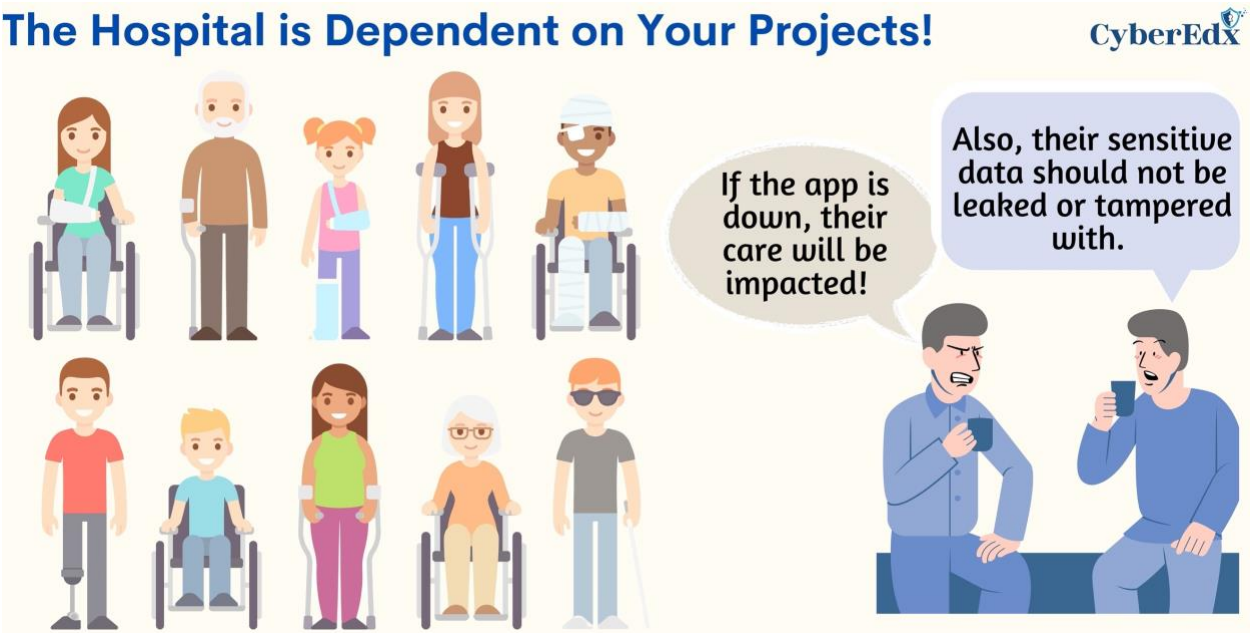

Figure 2.3: Patients dependent on your "My Health" application

Let's try to understand some basic security terms in the context of this case study. We'll name this project "My Health." Let's call the app "My Health."

In this section, we'll go over three fundamental security principles. They are referred to as the CIA Triad. Make sure not to confuse this with the Central Intelligence Agency of the USA.

The 3 Pillars of the CIA Triad are:

- Confidentiality
- Integrity
- Availability

Let's discuss these in detail.

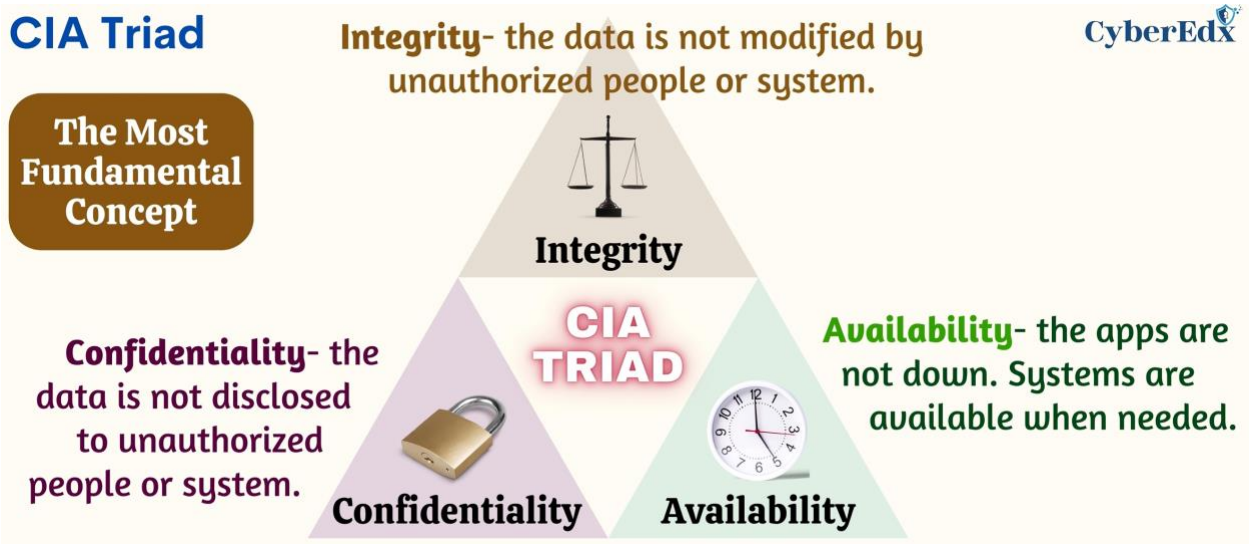

Figure 2.4: The three pillars of the CIA Triad

Confidentiality

The protection of data from unauthorized access is referred to as **confidentiality**. It is about ensuring that no **confidential** information is disclosed to people who are not authorized to see it.

Our case study "My Health" project will deal with personal patient health information as well as other data like their name, age, SSN, Insurance-ID, doctor's findings, and more.

Would the patients be willing to share this information with the hospital personnel? Of course, Yes! Otherwise, how else would they be able to receive the care they require? But should this information be shared with someone else? It really comes down to who this "someone else" is.

Why? This is mainly because you wouldn't want the rest of the world to know about a patient's personal information and health problems. This is private data that should be kept safe and in the right hands. And in the case of health records, it is anyway against the law to share medical information without the patient's consent, and violating this law could subject you to hefty fines and penalties.

Whatever industry you work in, your products will deal with sensitive customer data that must be safeguarded. The customer-sensitive data could include customer names, home addresses, payment card information, social security numbers, emails, and more.

Confidentiality entails keeping sensitive data accessible only to those who need to know it and inaccessible to all others.

Figure 2.5: Confidentiality explained

It's important for you to know what data your products will be collecting and how that data will be used. It's also your responsibility to ensure that confidential data is protected.

Let's talk about the current projects you are working on. We have some questions for you to consider:

- What data is collected in your projects?
- How much of that data is sensitive? Or regulated?
- How and where the data is stored? Who has access to the data?
- Is the sensitive data encrypted at all times, during storage and transit?

Here is a sample of what data is confidential:

- **PII** - Personal Identifiable Information (name, address, birth date, etc.)
- **PCI** - Payment Card Industry (payment card number, expiry date, etc.)
- **PHI** - Personal Health Information (patient's name, address, birth date, hospital admittance, discharge dates, etc.)

Frameworks like HIPAA (Health Information Portability & Accountability Act) have regulations to identify what data is considered sensitive or restricted. HIPAA applies to the healthcare industry and may not be relevant for you. However, it is imperative for you to find out what security regulations or standards apply to your industry and your projects. We'll talk about the regulations and standards in the following chapters.

In most projects, business specialists and product owners provide answers to questions about what data is confidential. They collaborate with the security and compliance teams to compile a list of confidential data pertinent to the project. It's important that the product and security teams collaborate, and you can play an important role in making that happen.

Figure 2.6: Your product and security teams collaborating

Integrity

Integrity is "Protection against unauthorized modification or destruction of information." [11] Assume a doctor has prescribed 100 mg of a particular medication to a patient on the "My Health" app. What if a hacker intercepts it while it's in transit from the My Health app to the pharmacy online system and tampers with it? He changes the value from 100 to 300 mg. For hackers, this isn't a big deal, but what about the patient? If the patient consumes 300 mg of medication instead of 100 mg, it may be detrimental

[11] https://csrc.nist.gov/glossary/term/integrity

to his/her health or even be life-threatening. Apart from endangering the patient's life, it might also result in public scrutiny, liability, and other consequences.

In a banking transaction of $10,000 to a foreign bank, imagine the repercussions of an attacker intercepting the data, removing one '0' at the end.

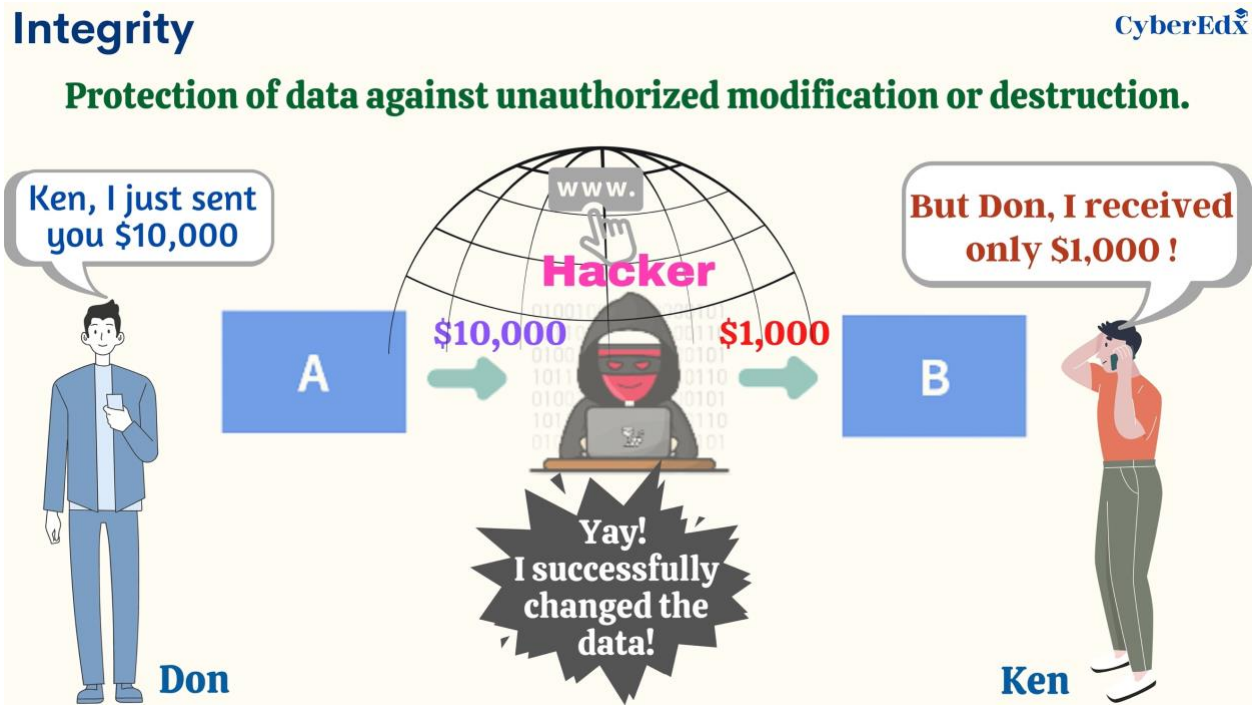

Figure 2.7: A hacker intercepting data and tampering with it

It's essential that recipients receive messages intact, or in other words, complete and unaltered. If a message is modified, it certainly loses its value and may, in fact, cause harm. The accuracy and completeness of data are what we call **integrity**.

Your applications may be dealing with important company and user data. You and your team need to ensure that the data in your applications is safe from unauthorized modification or deletion.

Availability

Availability means that authorized users will have access to the systems and the resources they need when they need them.

Assume the patient uses the "My Health" app to renew medications and communicate with their care team, but the app is down. This could be due to servers failing or systems being shut down because of cyberattacks or some poor coding. Regardless of

the reason, the users won't be able to access the application when they need it, and this may impact their care.

In October 2021, Atento, a multinational business process outsourcing company, was hit by a cyberattack, with the greatest impact seen in Brazil. The attack disrupted service for its clients, which included major global banks.

There is a type of cyber-attack where an attacker floods a website, server, or network with an overwhelming amount of traffic or requests. This excessive traffic or requests can overload the system, causing it to slow down, crash or become unavailable to legitimate users. This type of attack is called a **Denial of Service (DoS)** attack. DoS attacks can impact availability by making it difficult or impossible for legitimate users to access a system or service.

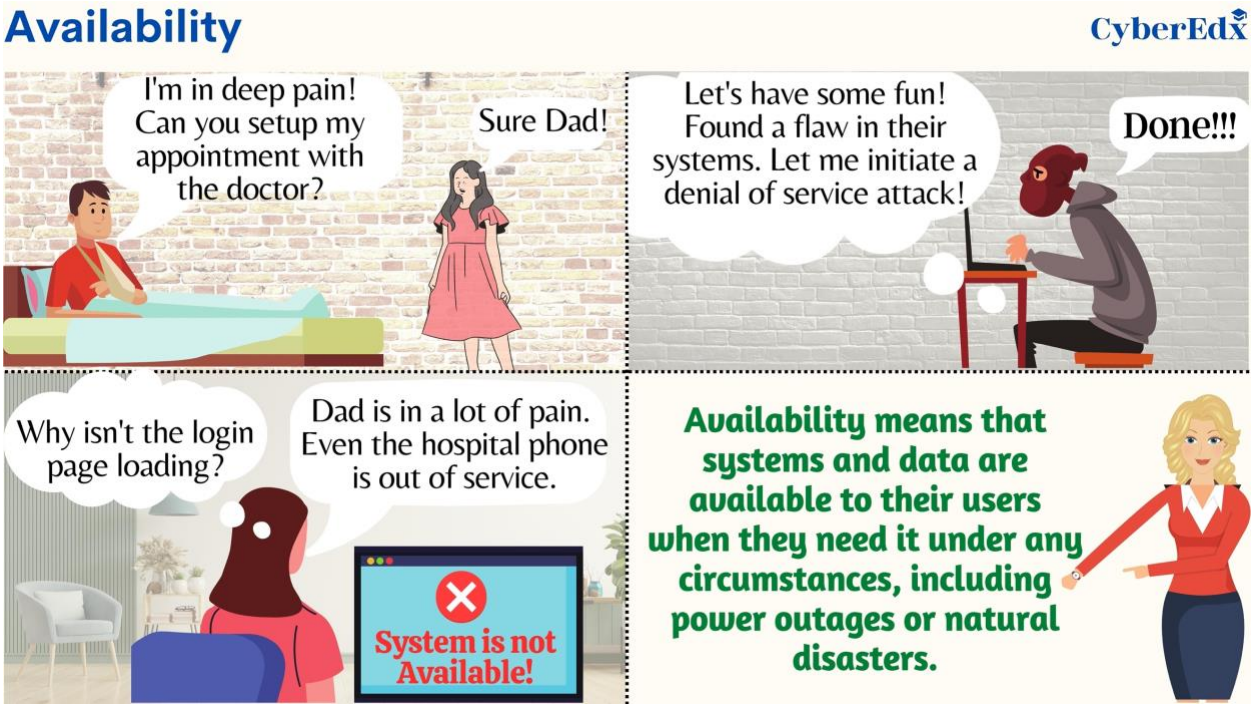

Figure 2.8: An attack on servers that makes the application unavailable

If there are availability issues with the "My Health" application, the care of the patients may be impacted. If a patient is in critical condition, it may lead to mishaps. Imagine that a patient needs surgery, but the patient's information is not available because the servers are down. It's important that the critical functions of your organization are available 24/7. Another thing to keep in mind is that availability is measured in 9s. If your system is up and running 99% of the time, we call it two-nines, 99.9%, three-nines, 99.99%, four-nines, and so on.

To summarize, **availability** ensures that all systems and applications are available to the users when needed by them. The systems must be protected from unintentional destruction, and information must be available when needed, even during holidays or natural disasters.

Exercise 2.1: Match the terms in Column A with those in Column B. The item in Column **A** results in the absence of the item in Column **B**.

Column A		Column B	
1	A healthcare professional updates patient data incorrectly by mistake	a	Confidentiality
2	A doctor cannot access a patient's data about past appointments		
3	Sensitive information of a customer is visible to another online	b	Integrity
4	A banking website is down		
5	Credit card data of a customer is obtained by a hacker through unauthorized means	c	Availability

Exercise 2.2:

Work with your team to determine what data your applications are collecting and how the data's confidentiality, integrity, and availability are maintained.

More Cybersecurity Terms

Here are some more basic security terms that we will use throughout this book.

Asset

An asset is anything that is valuable, useful, and must be protected.

Look around you. Is there anything that you consider to be valuable? Household assets might include your laptop, phone, furniture, documents with sensitive information, and

other items you would deem confidential. Here are some examples of your organization's assets:

- **Physical devices:** laptops, tablets, smartphones, and essentially any device that your team uses to access company and customer data.
- **Software:** mobile apps, websites, employee applications, and the application your team is currently developing.
- **Data:** customer data, company data, and even project data, including user stories, requirements, product backlogs, and any other information created and used in your project.
- Finally, assets also include **work locations** such as the company's office, hospitals, server rooms, data centers, meeting rooms, and your home office.

Assets must be safeguarded against attacks or unauthorized access. You should be aware of the assets your project will be using. You may have to procure assets specifically for your projects. For example, for the "My Health" project you would have to procure some smartphones and IoT devices to test the application. In addition to physical items, you should also be aware of the data that will be used and created.

Threat

A threat is any person or event that can impact an asset's confidentiality, availability, or integrity. Imagine a bear in the jungle, a malicious gunman, or a burglar. They are all threats to your physical security, aren't they? An unidentified person roaming around your house is possibly a potential threat.

Figure 2.9: An example of threat

Now let's shift our focus to organizational threats. Cybercriminals may attempt to obtain your team members' credentials. Their goal may be to gain access to customer and company information. They may try to find some weaknesses in your applications to get access to sensitive data. Here, cybercriminals are a potential threat to your organization.

A former employee with access to your servers may try to access the sensitive data. Here, the former employee is a threat. You must be aware of the potential threats. As we progress through this book, we'll take a close look at the various types of threats.

Risk

The possibility that something detrimental will occur is referred to as risk. Consider the following scenario: you have completely secured your home, but one of your windows was open or broken. This would be an ideal opportunity for a thief to break in and steal your belongings. The risks of this are:

- financial loss
- your personal information falling into the hands of an individual with malicious intentions.

Figure 2.10: A few examples of risks

In your organization, your customers' sensitive data may fall into the hands of hackers. The hackers could expose the information on social media, jeopardizing the organization's reputation. It could render financial consequences as well, as the company may be fined for data theft. Some companies require employees to complete security training, but contractors are not required to do so. Due to their ignorance, contractors may introduce vulnerabilities in the applications, which is a risk.

Risk management is important; the better you manage security and compliance risks, the less likely it is that your organization will be a victim of cyberattacks and data breaches. In the next chapter, we will go over the risks you should watch out for.

Vulnerability

A vulnerability is defined as a flaw or weakness in the design or implementation of an asset that could be exploited by a threat.[12] An open or broken window in your home is a vulnerability because a thief can use it to gain entry. An employee who does not lock the workstation when leaving the desk is one example of a vulnerability.

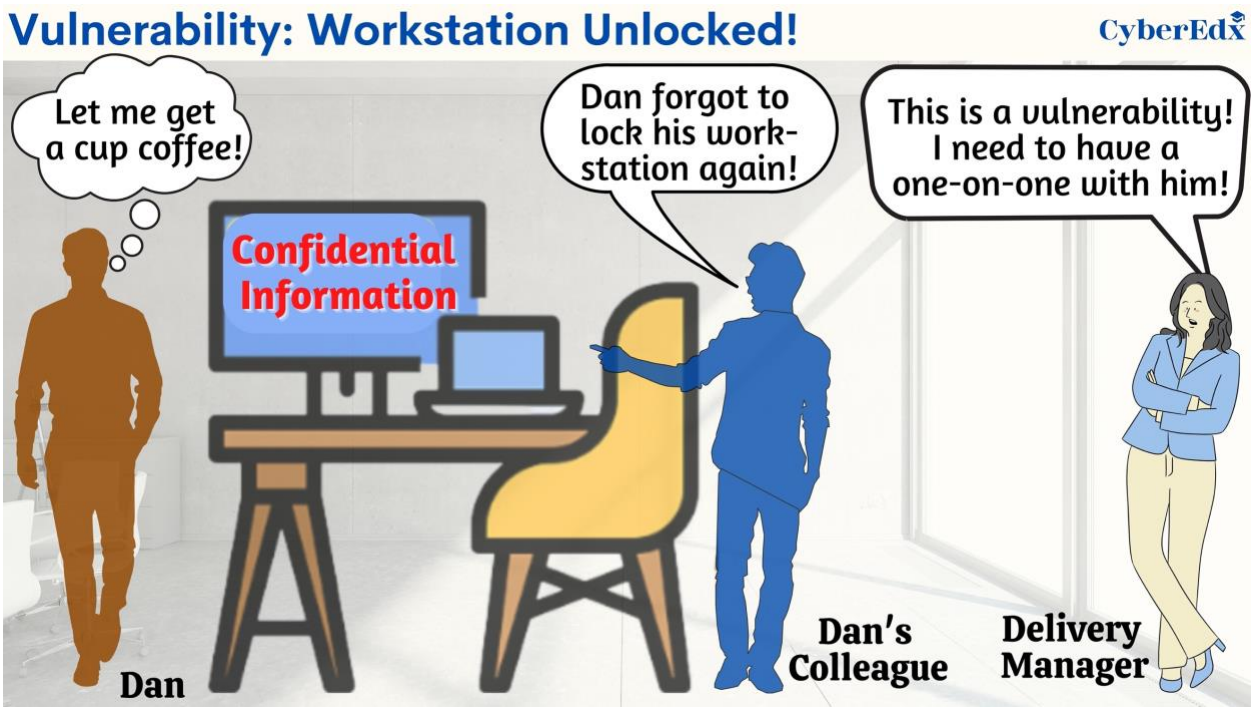

Figure 2.11: Vulnerability – Team member leaving the workstation unlocked

[12] https://en.wikipedia.org/wiki/Vulnerability_(computing)

In our case study, the "My Health" application, a vulnerability could be a design or coding flaw that allows an intruder to access the application.

People with malicious intent are always on the lookout for a flaw or loophole in the system. Something as simple as using an old version of an operating system or utility can allow a hacker to gain entry to data, networks, and systems. Many times, a security flaw is fixed in a newer version of the operating system, but the user is still on the older version. This resulted in the infamous WannaCry breach of 2017. There may also be vulnerabilities in third-party software used by your applications that your team should be aware of. It is critical that your project does not introduce any new vulnerabilities and that existing ones are identified and fixed as soon as possible.

Breach

When an intruder gains access to an organization's protected systems and data, it's referred to as a breach. For example, a breach happens when the attacker gets unauthorized access to email accounts, laptops, servers, or computer networks.

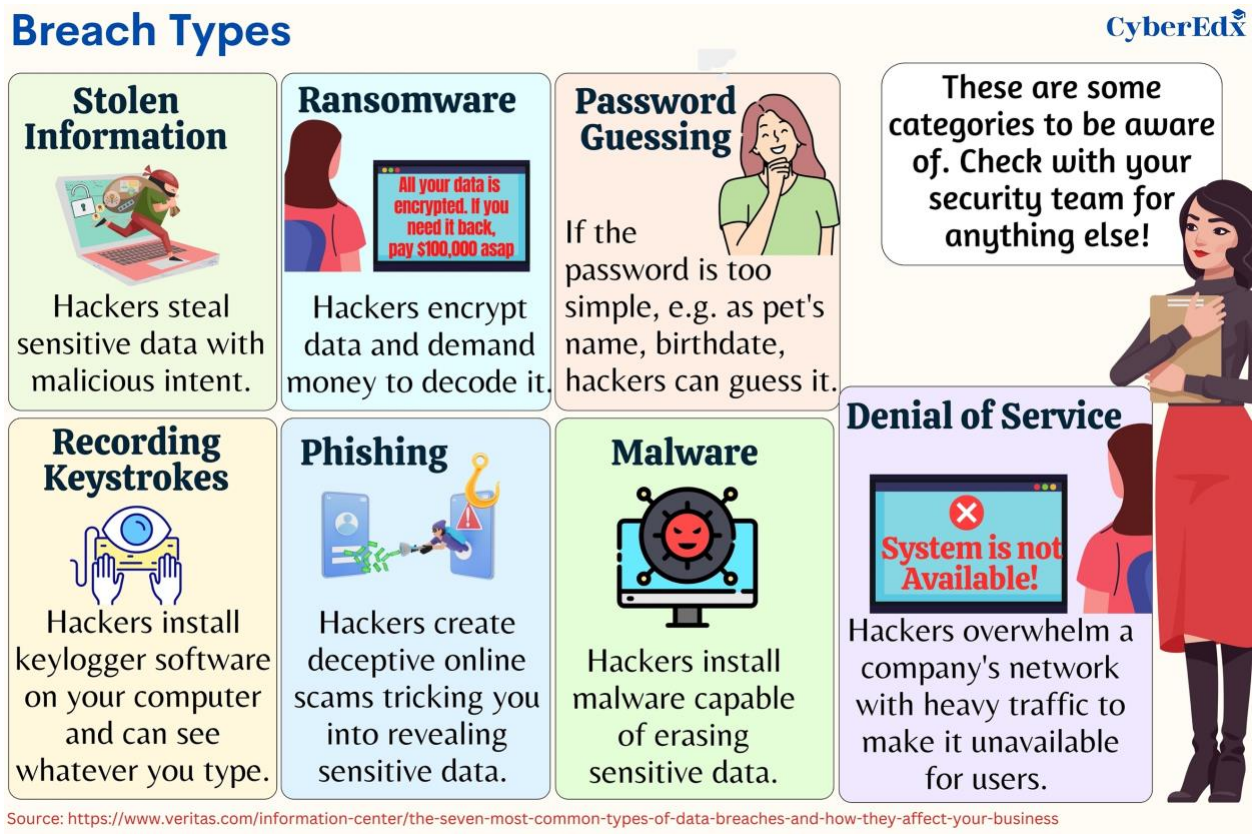

Figure 2.12: Some types of breaches to keep an eye on

The infamous SolarWinds breach in 2020 exposed the sensitive data of top government agencies and large organizations. SolarWinds is a software company, which provides tools for network and infrastructure monitoring, and other technical services to hundreds of thousands of organizations around the world. The hackers were able to attach malicious software to SolarWinds software updates. More than 18,000 SolarWinds customers, including top government agencies, installed the malicious updates, with the malware spreading undetected. Through this code, hackers accessed SolarWinds's customer information technology systems containing sensitive information.[13]

CSO Online observes: "Not long ago, a data breach affecting a few million people would have made headlines. Breaches affecting hundreds of millions or even billions of people are now far too common."

In our example "My Health" application, a breach occurs if an intruder gains access to patient data. An understanding of potential breaches will help your team collaborate with security professionals to build applications that are robust and free from vulnerabilities. The understanding of the security risks will help you manage these effectively.

Exercise 2.3: Match the terms in Column A with those in Column B.

Column A		Column B	
1	Theft of intellectual property	a	Asset
2	Laptops provided to developers	b	Threat
3	A hacker trying to get unauthorized access to credit card data	c	Risk
4	Lack of security training for the contractors	d	Vulnerability
5	Security defect in a software program running in production	e	Breach

Encryption

Encryption is the process of converting data into a secret code in order to keep sensitive information hidden from unauthorized people or systems.[14]

[13] https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[14] https://www.techtarget.com/searchsecurity/definition/encryption

Do you recall making up secret languages as a kid? Your close friend could understand all your gibberish words. Your other buddies, on the other hand, had no idea what you were talking about. You figured out specific codes that only you and your friend could decode. To put it another way, you have encrypted your words. The encrypted language you were using was meaningless to your other friends.

Encryption is the process of transforming data into secret codes so that the information is of no use to unrelated people or systems. Converting an encrypted message back to its original form is referred to as **decryption**. In your organization, you encrypt sensitive data to prevent it from any misuse. Before you send the sensitive data from your servers to its users, it is encrypted. Your receiver, who is your genuine user, has that secret code to decrypt the data to its original form.

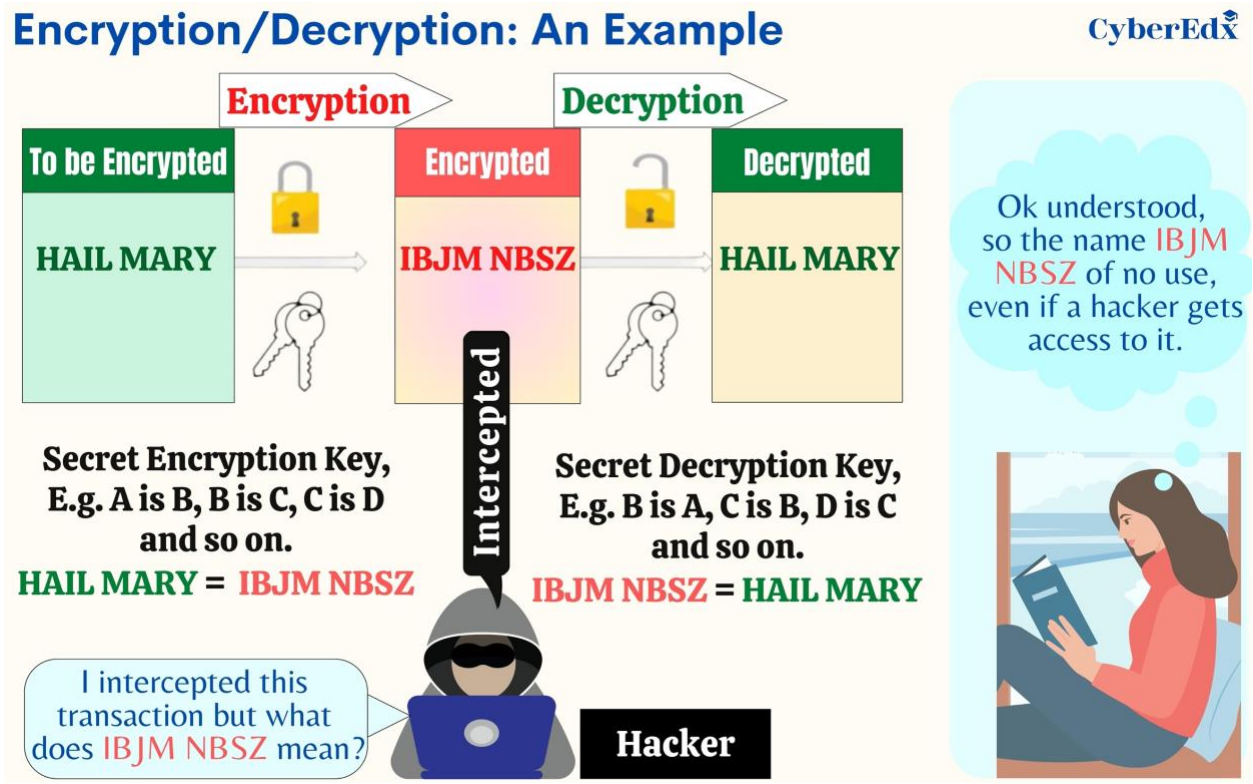

Figure 2.13: An example of encryption and decryption

The variable value applied using an algorithm to encrypt data is called an **encryption key**. On the other hand, the variable value applied using an algorithm that converts the encrypted data back to its meaningful form is called a **decryption key**. The process of encryption and decryption is referred to as **cryptography**.

Identity and Access Management

Identity and Access Management (IAM) is a collective term that covers products, processes, and policies used to manage user identities and regulate user access within an organization.[15]

Let's look at both identity and access management in more detail.

Identity

Identity is who you are. When you travel, you must present your ticket and an ID card, which may be a driver's license, passport, or any other acceptable picture ID. Airlines use this method to ensure that the ticket was issued to "you"' and that "you"' are the one traveling, not someone else.

Now, let's discuss who controls your ID. If it's your passport, the passport issuing authorities ensure that it is yours and only yours by examining the information in your application, supporting papers, background checks, and so on. As a result, passport issuing authorities manage your identity.

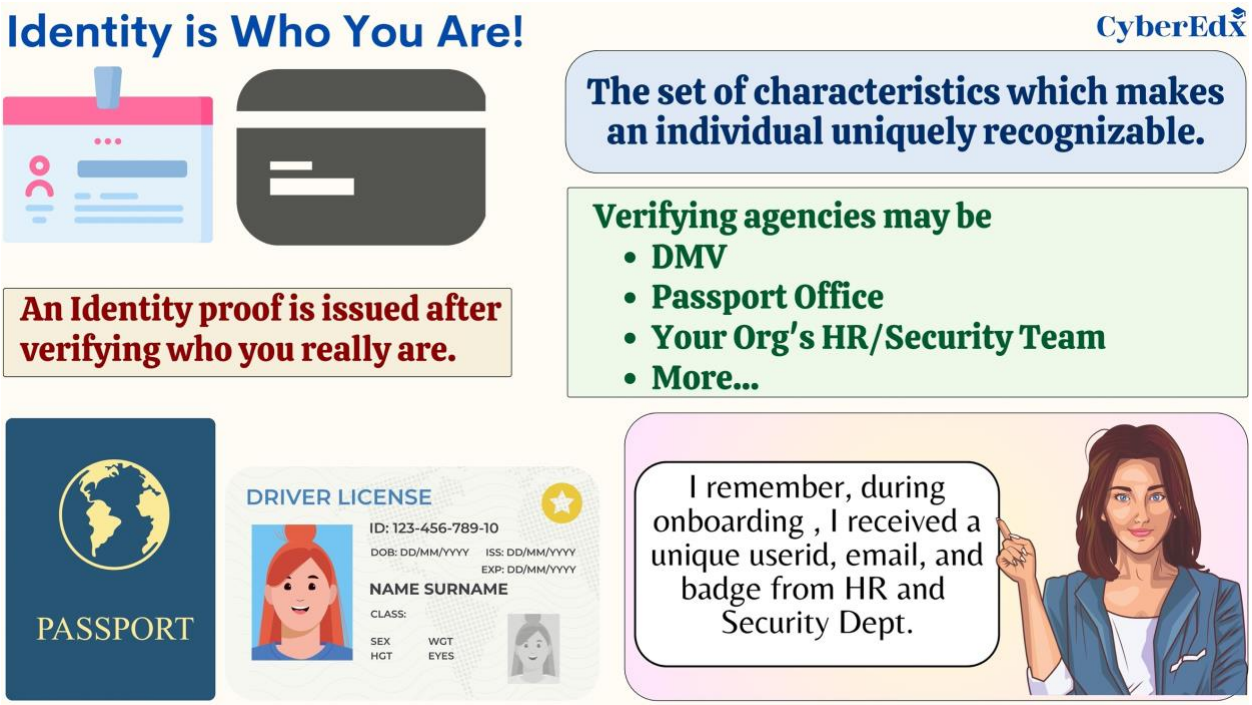

Figure 2.14: Your identity is unique

The identity management team in your company is responsible for providing identities to all users. When you join a new company, you are provided a user id to login into

[15] https://digitalguardian.com/blog/what-identity-and-access-management-iam#

your work computers by the identity management team. In other words, **identity** is a set of characteristics which makes an individual uniquely recognizable.

Access Management

Access management is defined as the process of only allowing authorized people or systems to access resources. Let's refer to our traveling example. Assume you bought a first-class ticket. When you enter the aircraft, the flight attendant checks if your ticket is economy or first class. If they find it valid, they will allow you to get into the first-class seating area. The flight attendant is performing access management by making sure that only authorized people (people with the correct tickets) can access first-class seating.

Similarly, not all team members will have access to all your organization's resources. You may not have access to the resources which an architect or a developer may have. A consultant may not have the same resources as a CEO, and vice versa.

Figure 2.15: Example of access management

Multi-Factor Authentication

Multi-factor authentication (MFA) is an authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) including:

- knowledge (something only the user knows),
- possession (something only the user has), or
- inherence (something only the user is)

MFA protects user data—which may include personal identification, personal health information or financial assets—from being accessed by an unauthorized third party that may have been able to discover, for example, a single password.

The authentication factors of a multi-factor authentication scheme may include:[2]

- Certain knowledge is only known to the user, such as a password, PIN, OTP (One Time Password), etc.
- Any physical object in the possession of the user, such as a security token, fob (small hardware device), a bank card, a key, etc.
- Some physical characteristics of the user (biometrics), such as a fingerprint, face, voice, etc.

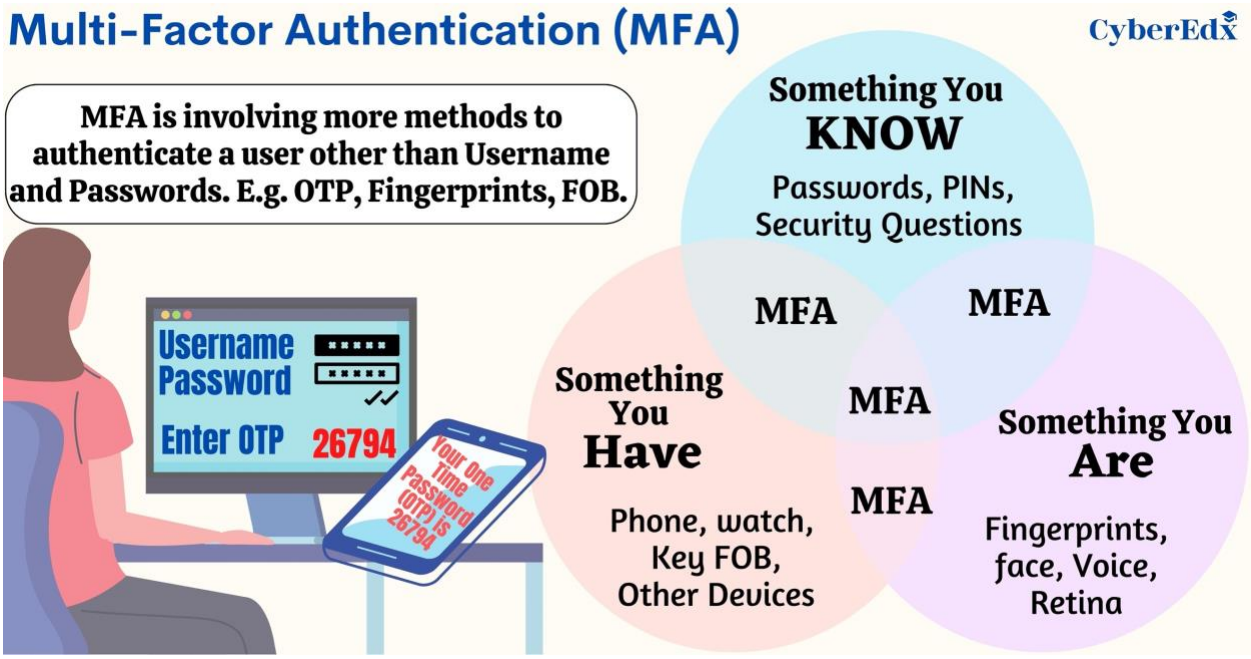

Figure 2.16: Multi-factor authentication and various authentication factors

It is difficult for users to remember and keep track of their passwords. It is preferable to use authentication factors other than passwords to identify users.

MFA can also help protect against credential stuffing attacks. What are credential stuffing attacks? **Credential stuffing** is a type of cyber-attack where attackers use automated tools to try different combinations of usernames and passwords on a website or application until they find a match. Credential stuffing is made possible by the fact that many people reuse the same username and password across multiple accounts, making it easier for attackers to gain access.

The most effective way to prevent credential stuffing attacks is using **passwordless authentication,** which is a type of authentication method that does not require a user to enter a password to access their account. It relies on alternative methods to verify a user's identity, such as biometrics, hardware keys, one-time codes sent via email or text, or other forms of multi-factor authentication.

Security Controls

A **security control** is a safeguard or countermeasure used to prevent, detect, mitigate, or reduce security risks to a company's assets. In other words, security controls prevent the chances that a vulnerability is created or reduce the chances of a threat exploiting a vulnerability. On a high level, there are three types of security controls used by companies: Technical controls, administrative controls, and physical controls.

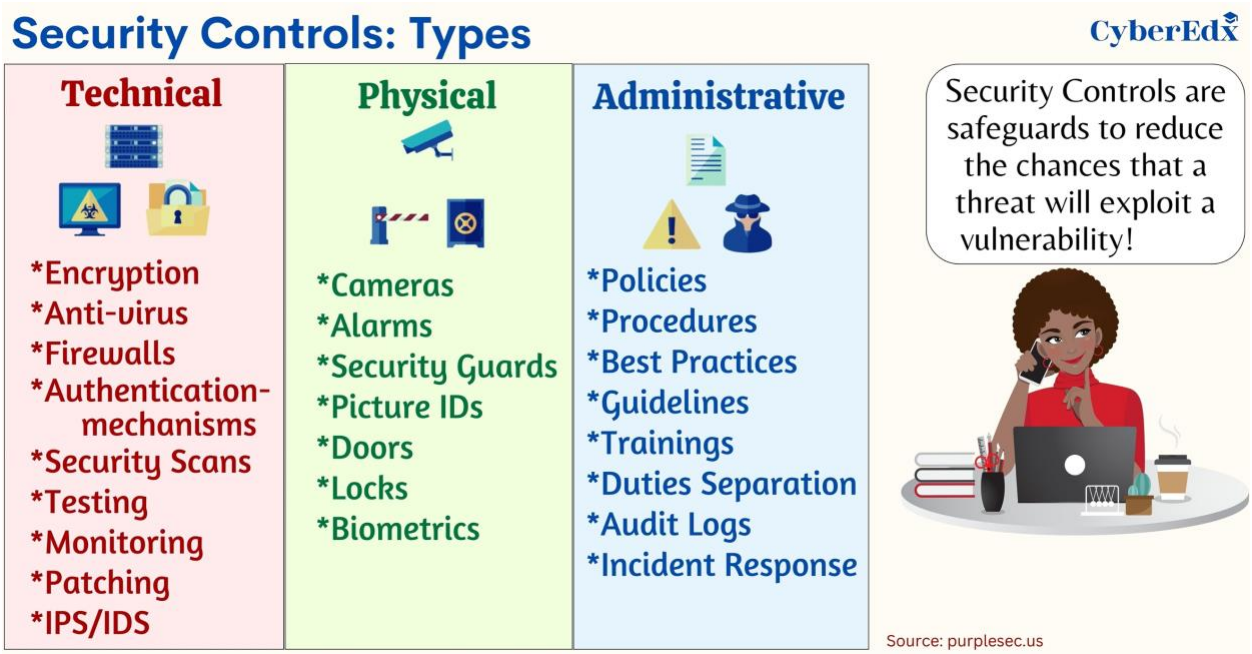

Figure 2.17: The various types of security controls[16] *Source: Purplesec*

Technical controls use software tools to protect hardware and software. Some examples of technical controls include encryption, antivirus software, firewalls, authentication mechanisms, IDS (Intrusion Detection Systems), IPS (Intrusion Prevention Systems). Antivirus software is used to protect assets from viruses and malware. A firewall is essentially the barrier that sits between a private internal network and the public internet.

[16] https://purplesec.us/security-controls/

Authentication mechanisms are put in place for verifying the identity of the user. IDS a monitoring system that detects suspicious activities and generates alerts. IPS continuously monitors a network for malicious activity and takes action to prevent it, including reporting, blocking, or dropping it, when it does occur. Security scans, testing, monitoring, and patching of the servers are some more examples of technical controls.

Physical controls are physical security measures to deter or prevent unauthorized access to sensitive material. Examples of physical controls are closed-circuit surveillance cameras, motion or thermal alarm systems, security guards, picture IDs, locked and dead-bolted steel doors, and biometrics (includes fingerprint, voice, face, iris, handwriting, and other automated methods used to recognize individuals)[17].

Administrative controls refer to policies, procedures, or guidelines that define personnel or business practices in accordance with the organization's security goals. Over time, organizations develop policies and procedures that have proven to be best practices. Every organization has different policies and procedures when it comes to security and privacy. For example, in some companies, it is a requirement that employees change their passwords every 5-6 weeks. Many companies prohibit their employees from accessing personal email accounts at work.

It is imperative that you find out about your company's policies and procedures for security and determine how they may impact your projects and products. [18] Separation of duties refers to an administrative control in which one employee performs coding or configuration while another reviews it. Other controls in this area include audit log review and incident response.

The security controls can also be classified as preventive, detective, or corrective.

- **Preventive controls** prevent the creation and exploitation of vulnerabilities.
- **Detective controls** alert the organization when an unauthorized activity occurs.
- **Corrective controls** correct or reduce the harmful activity from further exploiting the vulnerability.

We'll cover preventive, detective, and corrective controls with examples in the following chapters.

[17] https://purplesec.us/security-controls/#Goals

[18] https://csrc.nist.gov/Projects/risk-management/sp800-53-controls

Offensive and Defensive Security

Offensive security, also known as "red teaming," is focused on attacking a system or organization to find weaknesses and vulnerabilities. This involves using the same tactics, techniques, and procedures that real attackers would use to test the security of a system. The goal of offensive security is to find weaknesses before real attackers can exploit them, so they can be fixed before any damage is done. Red teams are a group of security experts who perform offensive security.

Defensive security, also known as "blue teaming," is focused on protecting a system or organization from attacks. This involves using tools and techniques to monitor the network and search for cyber threats that might otherwise remain undetected, also called threat hunting. The blue team also investigates and responds to security incidents. The goal of defensive security is to prevent attacks and minimize damage when attacks do occur. Blue teams are security experts who take care of defensive security.

A **purple team** is a combination of a red team and a blue team. The purple team approach combines the offensive and defensive capabilities of both the red and blue teams to improve an organization's overall security posture.

All the teams work together to improve the security of a system or organization. Figure 2.18 lists the responsibilities of red, blue, and purple teams.

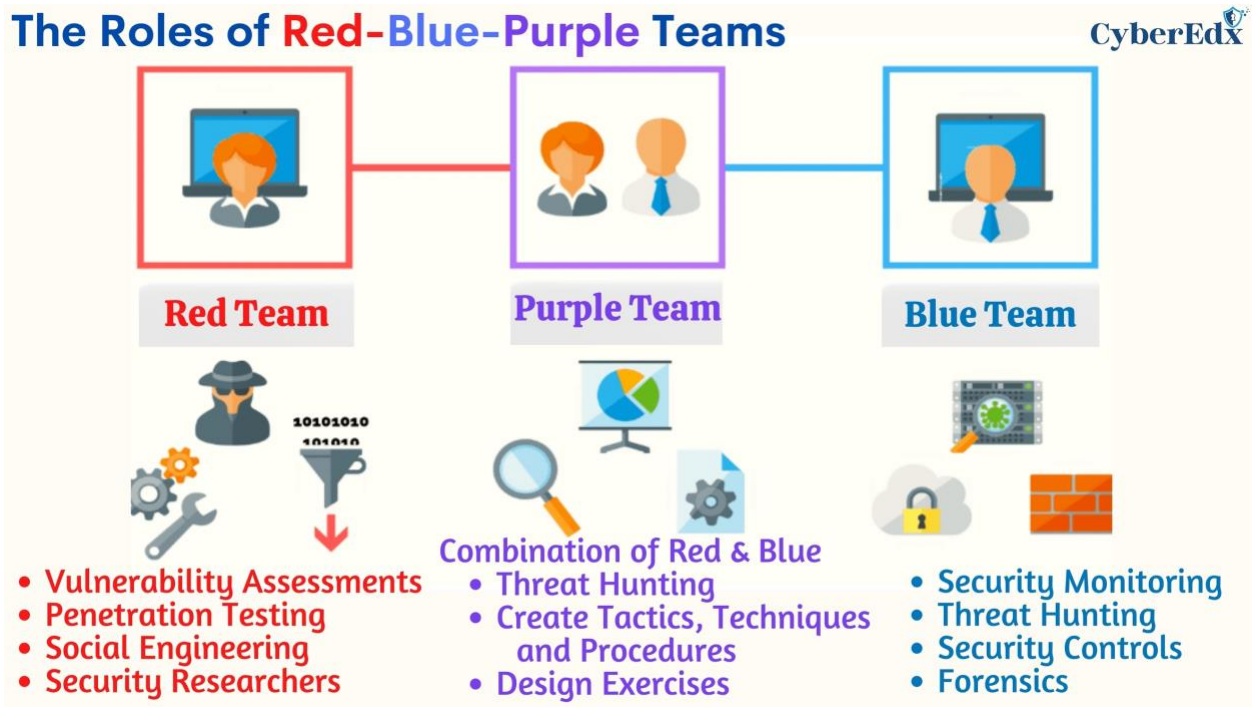

Figure 2.18: Roles of various teams explained

Defense in Depth

Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered to protect valuable data and information.[19]

A defensive mechanism is any tool, service, or system that lowers the risk of attack on an asset by intentionally getting in the way of the threat. A layered approach avoids a single point of failure.[20]

If one mechanism fails, another one steps up immediately to thwart an attack. One of the most effective ways to ensure confidentiality, integrity, and availability of assets is to take a defense-in-depth approach.

This is similar to the previous chapter's house example. In a house, the first layer of security is the lock on the front door. A monitoring camera could be used as a second layer. If a thief gets into the house, a third layer could be a sensor that sets off alarms. A fourth layer could be a phone call to the police. These layers together protect your valuable assets in your house. Businesses are increasingly implementing defense in depth to protect critical data from a variety of cyberthreats.

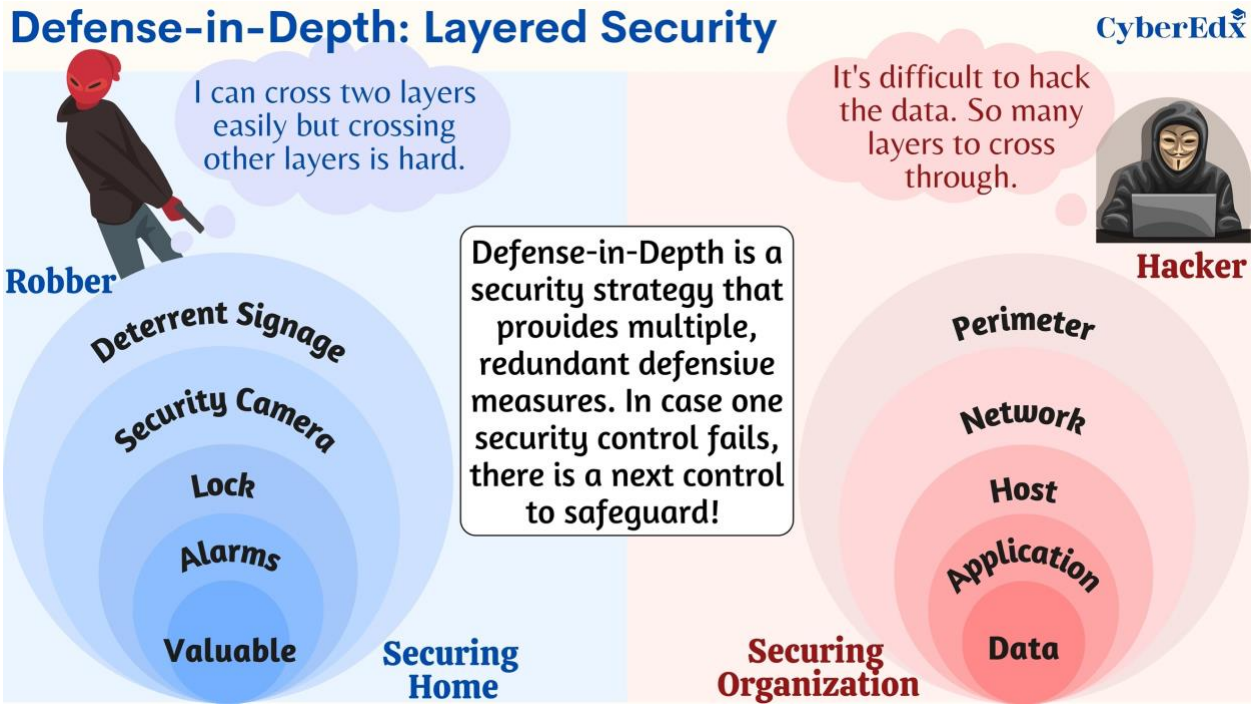

Figure 2.19: Defense in depth explained

[19] forcepoint.com/cyber-edu/defense-depth

[20] Virtue, Timothy, Rainey Justin "HCISPP Study Guide", Syngress

Non-repudiation

It is a security principle that refers to the ability to prove that a particular action or event has taken place and that the parties involved cannot deny their involvement.

The sender of a message cannot deny having sent it, and the recipient cannot deny having received it.

An example of non-repudiation in action would be David sending an email to Tony. Using cryptography, a digital signature is attached as part of the email. Tony can verify that the email was indeed sent by David. If David later tries to deny having sent the email, the Tony can use the digital signature to prove that the email did indeed come from David.

This helps to establish trust between the parties and provides a means of accountability, which can be important in a variety of contexts, including legal and financial transactions. To summarize, **non-repudiation** is a cybersecurity technique for trust. When there is evidence that you did something online, you cannot claim that you did not do it.

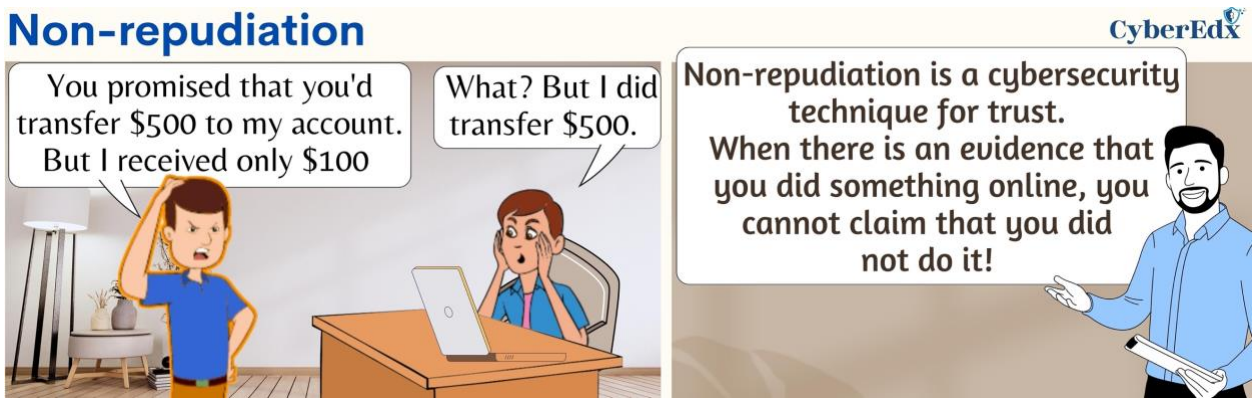

Figure 2.20: Non-repudiation example

Computer Networking

The majority of cybercrimes occur due to network-related issues. When your data travels through a network, it becomes vulnerable to manipulation.

A **computer network** is a system that connects multiple computing devices to transmit and share information. Isolated computers have limited value; they must work together to solve problems. Computer networks serve a variety of purposes, which include communication, file sharing, printing, and internet access. There are various types of computer networks, including:

- Local area networks (LANs) for small areas like homes, offices, or schools.
- Wide area networks (WANs) for larger areas such as cities, states, or countries.
- Internet is the world's largest computer network, connecting millions of computers globally.