Introduction

Mohammad Humayun Kabir

Head of Security Operations

Enterprise Security Management | Technology

Grameenphone Ltd.

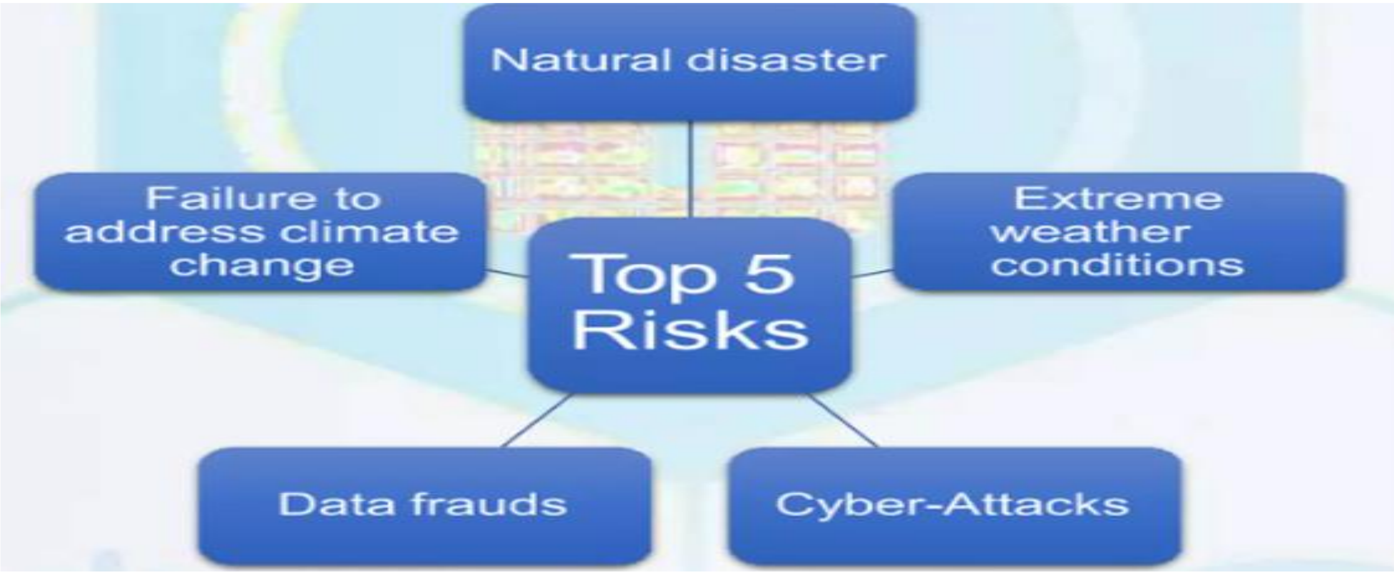
Your Cybersecurity Journey Starts Here

- Welcome, future defenders of the digital world!
- Explore one of the fastest-growing, high-demand, and impactful careers in the digital age.

- This session will guide you through :
  - why cybersecurity matters,
  - what opportunities await you,
  - how you can step confidently into a powerful and rewarding career,
  - what cybersecurity is,
  - CIA Triad,
  - Different Type of Attacks

Why Cybersecurity Matters

- According to the World Economic Forum, cybersecurity is now one of the top 5 global risks, right next to climate change and natural disasters. It’s a national security issue, an economic issue, and a personal issue. Cyber threats are rising globally, one threat ends, another one arises.



Why Cybersecurity Matters

- Every industry needs protection: finance, healthcare, telecom, government etc.
- Cybersecurity protects people, privacy, businesses, and even lives.
- It’s not just about tech — it’s about safety in a connected world.

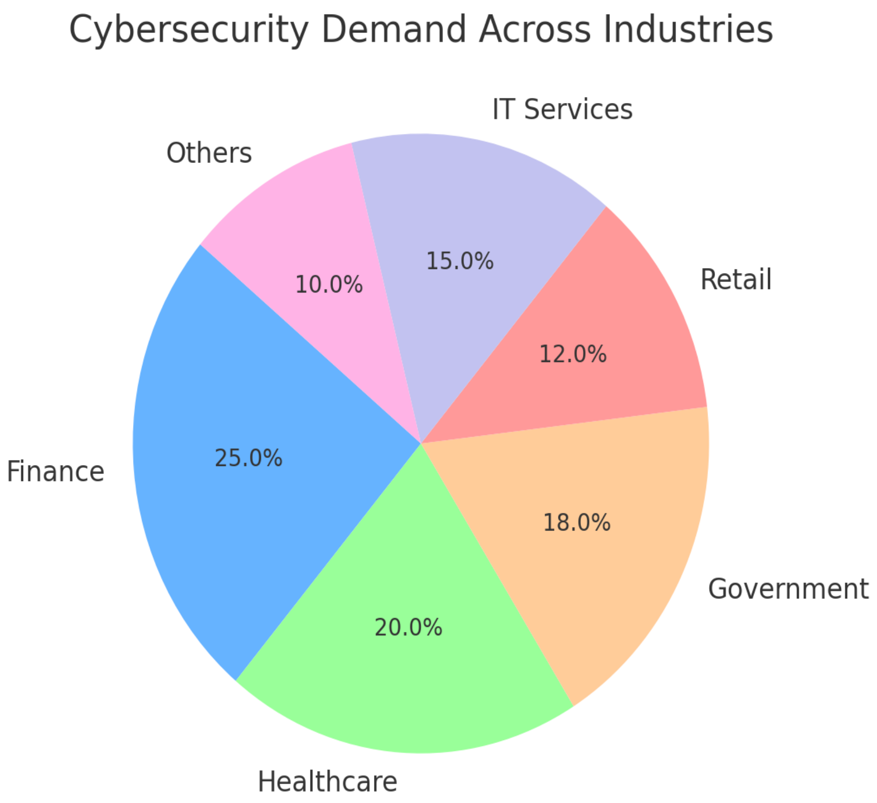
- Think about your phone. If someone stole it, maybe you lose a device. But if someone hacked it, they might drain your bank account, impersonate you on social media, or stalk your location.

- Imagine a classmate’s Instagram hacked. Or your parents tricked into sending money by a scammer. Or a hospital unable to access medical records because of ransomware.

The threats are real. And they don’t just cost money — they cost trust, privacy, and sometimes even lives.

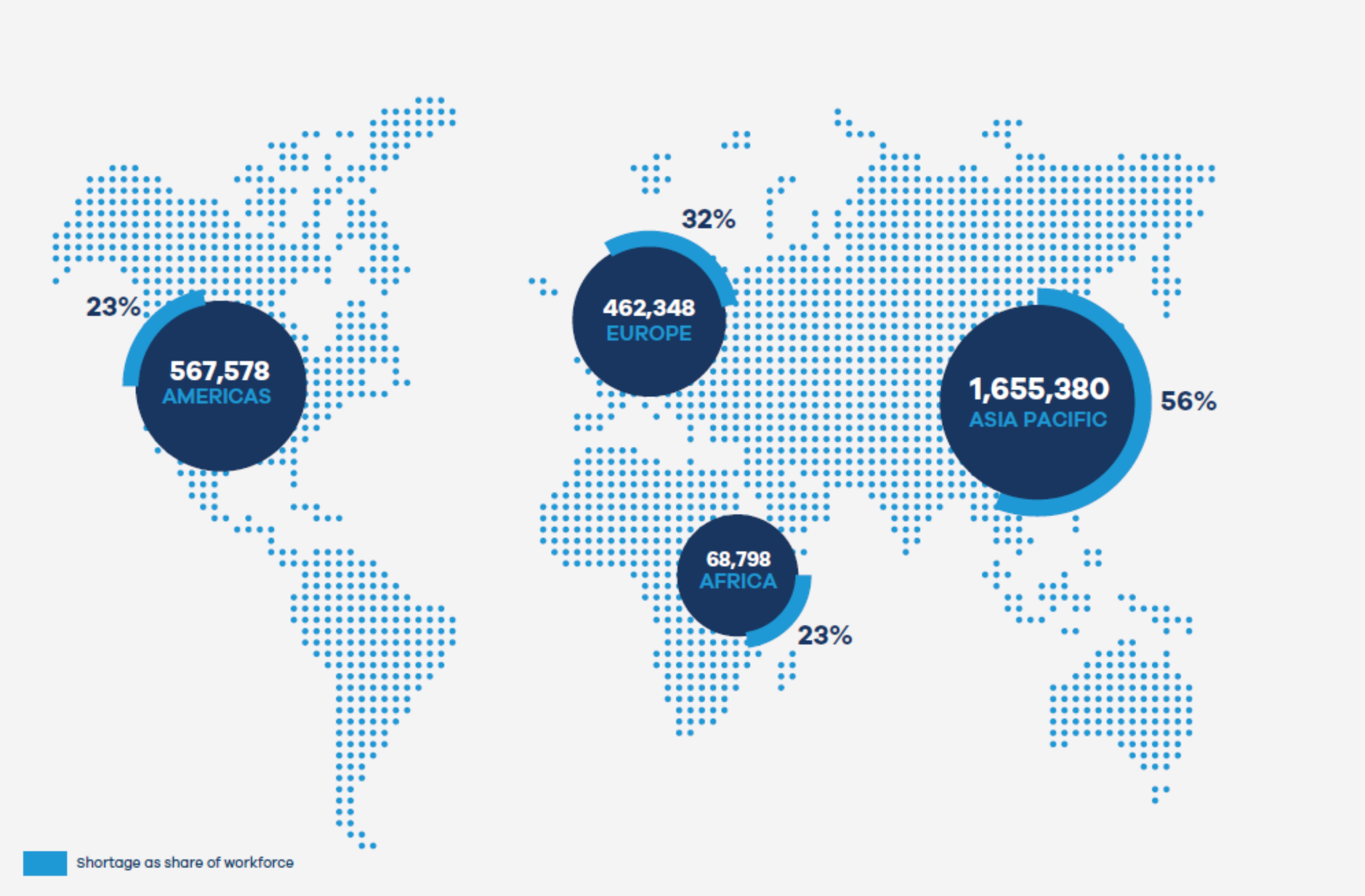
Skill Gaps, Opportunities & Career Path

Cybersecurity Demand Across Industries

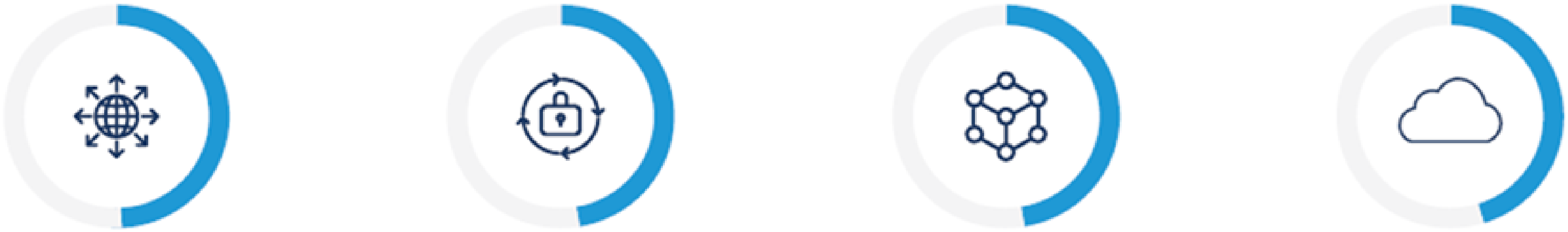


Right now, there are over three and a half million unfilled cybersecurity jobs worldwide. And that number doesn’t come from a blog or a rumor — it’s straight from industry research that governments, CEOs, and boards of directors take very seriously.

Regional view of workforce shortage



Most Challenging skills to be found



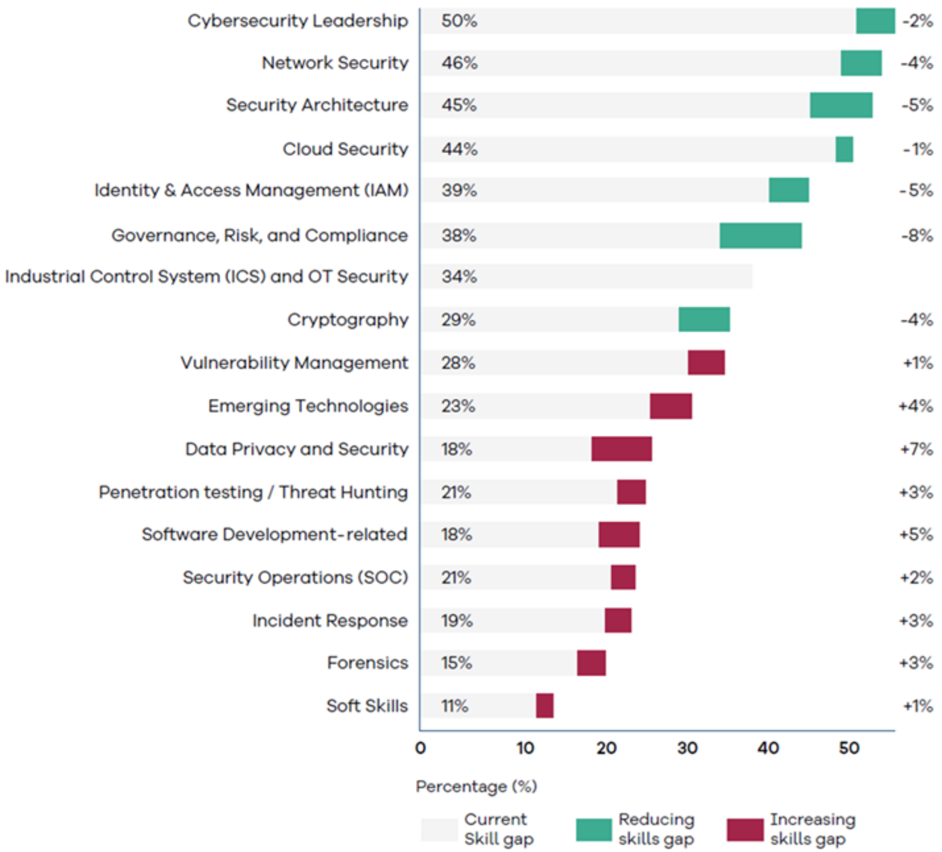
50%
Cybersecurity Leadership

46%
Network Security

46%
Security Architecture

44%
Cloud Security

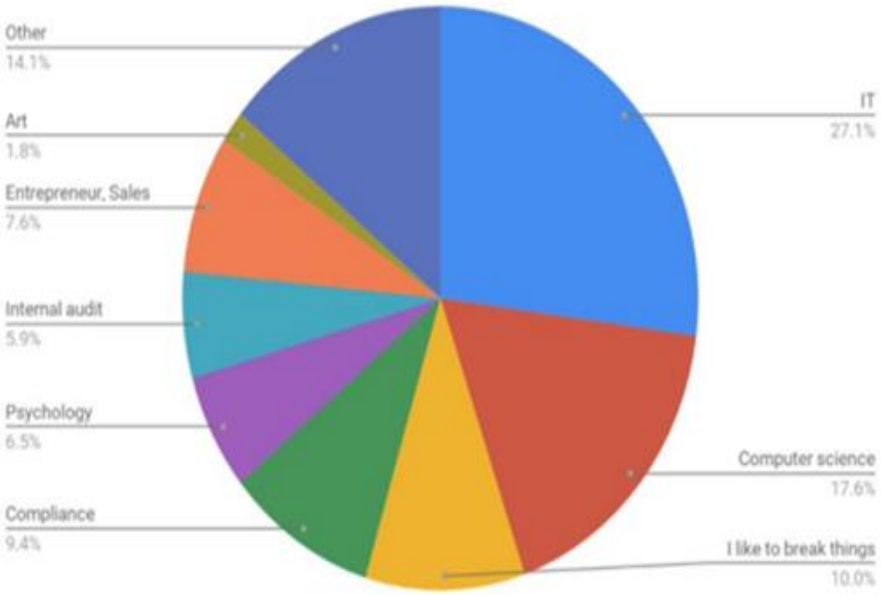
Expected skill gap in next 5 years



44%

Cloud Security

Cyber Welcomes All background



Close to 50% came from IT/CS.
Cybersecurity pros also come from:

- Psychology
- Compliance
- Art & Sales
- Internal Audit

If you're curious, driven, and love solving puzzles, this is for you!

Domains & Career Pathways in Cybersecurity

Domains under Cyber Security

- Application/Software Security
- Network Security
- Data Protection/Privacy
- Data Centre Security
- Legal/Regulatory Compliances
- Business Continuity/Disaster Recovery
- Cloud Security
- Digital Forensics

Domain under Cybersecurity

application and software security: Every mobile app you use — WhatsApp, banking apps, food delivery apps — has millions of lines of code. Hidden inside could be vulnerabilities waiting to be exploited. Application security specialists are like the quality inspectors of the digital world, making sure the code doesn’t betray its users.

network security. Imagine the internet as a massive highway system. Network defenders are the traffic cops, the gatekeepers, the patrol units. They keep out intruders, spot malicious traffic, and make sure communication flows safely from one end to another.

Domain under Cybersecurity

data/privacy protection: Data is the new oil, the new gold. Protecting it isn’t just about encryption — it’s about ensuring privacy, ownership, and trust. A data protection expert is the one making sure your medical record isn’t sold on the dark web, or your credit card details aren’t stolen in transit.

data center security: These are the fortresses of the digital age — massive buildings filled with servers that run the cloud. Imagine being responsible for protecting the very core of a nation’s financial transactions or telecom backbone. Physical guards, cameras, access controls — but also virtual defenses to keep intruders out.

Domain under Cybersecurity

legal and regulatory compliance: You may not write code or configure firewalls, but you shape the battlefield through rules. Compliance specialists ensure companies follow laws like GDPR, HIPAA, or local regulations. Break the rules? Fines in the billions. This is cybersecurity through the lens of law.

business continuity and disaster recovery: Imagine a hurricane takes out a data center. Or ransomware locks down a hospital. BCP and DR specialists make sure the business doesn’t collapse. They design backup plans, failover systems, and recovery strategies. They’re the ones who make sure the lights come back on.

Domain under Cybersecurity

cloud security: Perhaps the fastest-growing domain today. Everyone is moving to AWS, Azure, Google Cloud. But here's the catch: who owns the security? The company or the provider? Cloud security specialists answer that. They design architectures that are resilient, compliant, and secure by design.

digital forensics: This is where cybersecurity meets CSI (crime scene investigation). After a breach, forensic experts come in to find out *how* it happened, *who* did it, and *what* was taken. They analyze logs, trace IPs, recover deleted files — building the evidence that can stand up in court.

Domain under Cybersecurity

SOC — Security Operations Center: These are the watchtowers of cyberspace, where analysts monitor dashboards 24/7. Alarms go off, alerts flash, analysts investigate: is this real, or just noise? SOC engineers and detection specialists are the first to spot and stop an ongoing attack.

Incident Responder (IR): When the alarm turns out to be real then IR team steps in. These are the firefighters of cybersecurity. They contain the breach, evict the attackers, patch the weaknesses, and restore confidence. The IR team turns chaos into order.

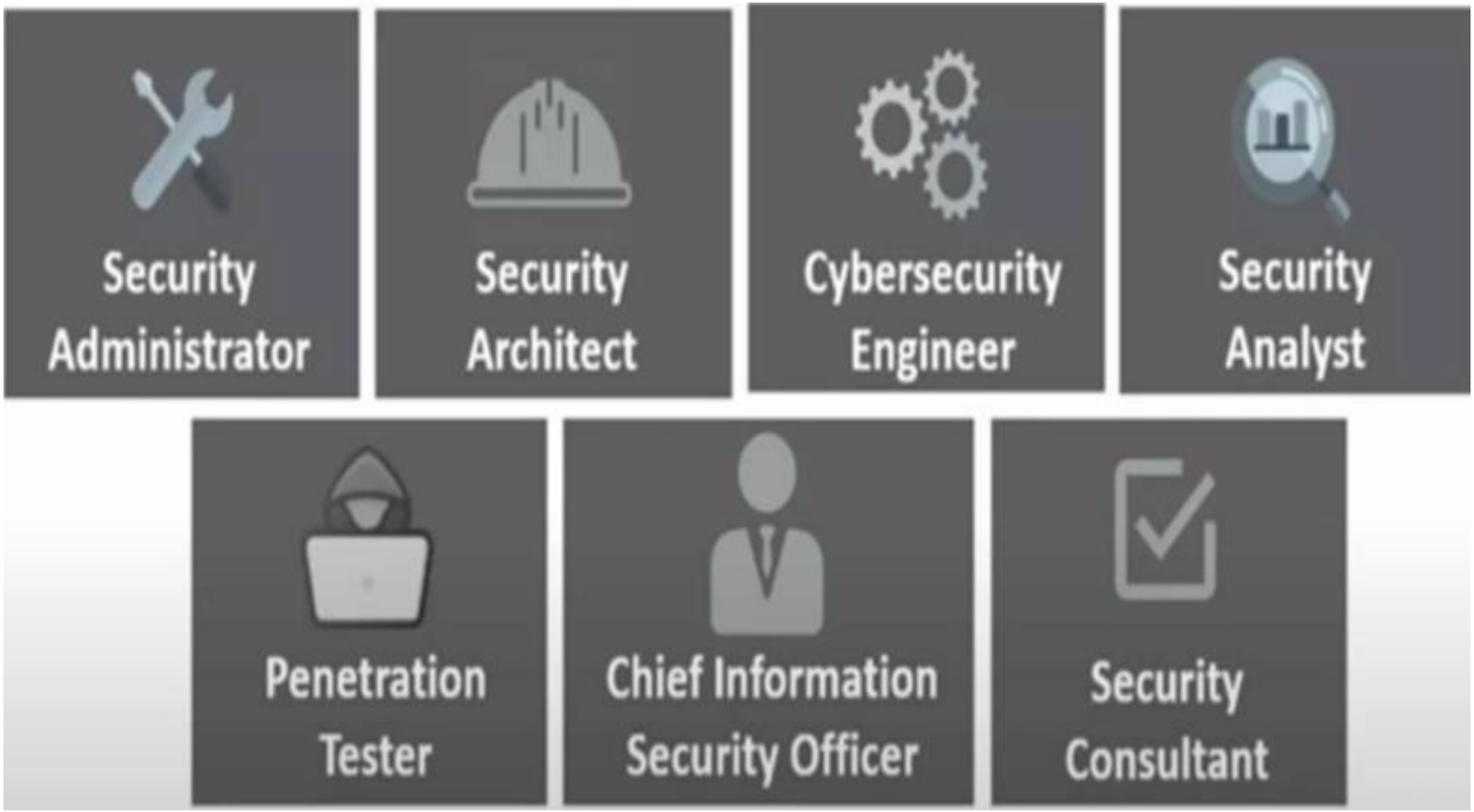
Domain under Cybersecurity

Each of these domains is a battlefield of its own. Some require coding, some require policy knowledge, some require investigative instinct. But all are crucial.

And here’s the beauty: you don’t have to pick your battlefield today. This course is your boot camp — you’ll get exposure to the concepts, the tools, and the mindsets.

Later, you’ll find your calling, whether it’s in code, in law, in forensics, or in leadership. Cybersecurity isn’t a single road. It’s a map — and today, you’ve just unfolded it.

Job Roles in Cyber Security



Security Administrator

Security Architect

Cybersecurity Engineer

Security Analyst

Penetration Tester

Chief Information Security Officer

Security Consultant

Cybersecurity Journey: Career Pathway

1. Entry Level: Security Analyst (learn fundamentals)
2. Intermediate: SOC Analyst, Incident Responder (tools & response)
3. Advanced: Pen Tester, Architect (offense & design)
4. Expert: CISO, Manager (strategy & leadership)

- At the entry level, you might start as a Security Analyst or SOC Analyst, you’re learning fundamentals.

- Then you can become a Penetration Tester, an Incident Responder, or a Forensics Investigator, analyzing logs, spotting threats.

- Later, you can move into leadership, mastery: designing secure systems, leading teams, creating strategy: Security Architect, Risk Manager, and finally, the top — Chief Information Security Officer (CISO).

Career Growth Example

- Year 1-2: Security Analyst
- Year 3-5: SOC Analyst / Pen Tester / Cloud Security
- Year 5-8: Cybersecurity Lead / Architect / Incident Manager
- Year 8+: Cybersecurity Manager /CISO / Cybersecurity Strategist / Consultant

Are You Ready to Be a Cyber Defender?

- The demand is high, the impact is global, and the field is exciting.
- Start now—be curious, stay sharp, and protect the future.
- Let’s build a safer digital world together.

- This course is your very first step into cybersecurity. Over the coming weeks, we’ll dive into the fundamentals — threats, security services, cryptography, authentication, even the emerging trends like AI in defense and zero trust security.

- You won’t just sit through theory. You’ll roll up your sleeves with labs, case studies, and a mini-project where you’ll design your own secure communication model.

- By the time we finish, you won’t just understand the concepts — you’ll have real, demonstrable skills. Skills you can put on your CV. Skills you can show off in interviews. Skills that employers are desperate to find.

Information Security & Cybersecurity

What is Cybersecurity?

- Cybersecurity is like a fortress—built with technology, process, people to guard against hackers and cybercriminals.
- It defends against criminal or unauthorized use of electronic information.
- Its mission is to ensure the safety of :
  - Data (what you store)
  - Identity (who you are)
  - Devices (what you use)
  - Networks (how you connect)

- Cybersecurity is all about keeping our digital world safe—just like locking the door of your house, but here we are locking information, networks, and devices.
- It’s like insurance, a guard dog, and a detective—all rolled into one.

Evolution of Security

- Physical Security – locks, seals, messengers
- Military/Diplomatic Security – Enigma, Code Talkers
- Commercial Security – ATMs, SSL, GSM
- Cyber Era – Cloud, IoT, Ransomware, Zero Trust

InfoSec vs NetSec vs Cybersecurity

- InfoSec → Protect data (any form)
- NetSec → Protect data in transit
- Cybersecurity → Protect digital systems, applications, and networks

Information Security (InfoSec):
Example: Keeping printed exam papers in a locked cabinet; encrypting sensitive customer data.
Network Security (NetSec):
Example: Firewalls blocking malicious traffic, VPNs securing remote connections.
Cybersecurity:
Covers both InfoSec + Network Security, but extends to applications, cloud, IoT, and user awareness.

InfoSec vs NetSec vs Cybersecurity

- **InfoSec = Protecting the treasure (data)**
- **Network Security = Protecting the roads (networks)**
- **Cybersecurity = Protecting the entire kingdom (overall digital environment)**

Importance of Cybersecurity in Daily Life

Cybersecurity is not just for companies—it impacts everyone.

Banking:

- Online banking transactions are protected with encryption.
- Cybersecurity prevents unauthorized transfers and fraud.

Social Media:

- Hackers may steal personal photos, impersonate you, or spread misinformation.
- Security measures like Multi-Factor Authentication (MFA) help protect accounts.

Business:

- Data breaches can lead to financial loss, reputation damage, and legal penalties.

Importance of Cybersecurity in Daily Life

Healthcare:

- Protecting electronic health records from ransomware and leaks.

Real-Life Analogy:

- Just like you lock your house doors every night, cybersecurity locks your digital doors to protect money, identity, and privacy.

CIA Triad

INTEGRITY
AVAILABILITY
CONFIDENTIALITY

Confidentiality: Protecting data from unauthorized access.

- Example: Using passwords, encryption, and access controls.
- Real-world: Banks use end-to-end encryption to keep your PIN secret.

Integrity: Ensuring data is accurate and not tampered with.

- Example: Digital signatures, checksums, hashing.
- Real-world: If someone changes your exam grade in the database, integrity is lost.

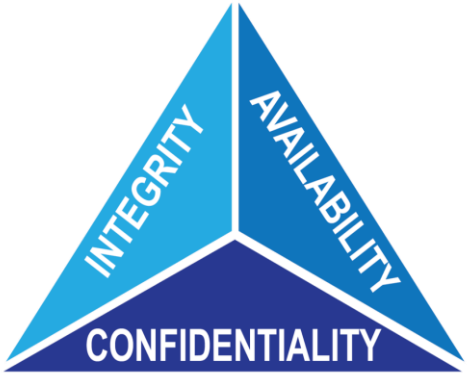
Availability: Ensuring systems and data are accessible when needed.

- Example: Redundant servers, backups, disaster recovery.
- Real-world: If an e-commerce site is down during a sale due to DDoS attack, availability is broken.

Opposite of CIA Triad is **DAD**

Disclosure, Alternation & Denial

CIA Triad



Think of a bank locker:

- **Confidentiality** = Only you and the bank have the key.
- **Integrity** = Bank keeps your money safe without altering it.
- **Availability** = You can access your locker whenever the bank is open.

CIA Triad

Examples from Telco:

Confidentiality — *SS7/Diameter Interception*

- **Story:** Signaling System 7 (SS7) and Diameter are protocols telcos use to set up calls, roaming, and billing. They were designed decades ago when only “trusted operators” had access.
- **What happened:** Attackers (or even shady operators) can exploit SS7 to intercept SMS (think one-time passwords for banking) or listen in on calls.
- **Impact:** Confidentiality of subscriber communication is broken. Real-world breaches have shown attackers silently eavesdropping on international roaming traffic.

CIA Triad

Integrity — Billing Manipulation / Fraud

Story: Diameter/SS7 messages carry billing and charging instructions. If an attacker alters those messages, they can reduce roaming charges, erase call records, or even charge someone else for expensive calls.

Example: In some fraud cases, attackers modified Call Detail Records (CDRs) so international calls appeared as local ones.

Impact: Direct financial loss for the operator, legal mess for customers.

CIA Triad

Availability — *DDoS on Core Network Elements*

Story: Telco networks rely on signaling gateways, HLR (subscriber databases), and media gateways. If these are flooded with bogus messages (a signaling storm or targeted DDoS), calls drop and mobile data stop working.

Example: A misconfigured IoT botnet flooded a European mobile operator’s Diameter network, causing partial outage.

Impact: Service unavailable for millions of customers.

Attacks – Passive & Active

Attacks are usually divided into two broad types — passive attacks and active attacks.

Passive Attacks – silent listening

- Eavesdropping: secretly listening to someone else’s private conversation.
- Traffic analysis: Even if data is encrypted, attacker watches who talks to whom.
- Telecom: IMSI catchers silently capture mobile identities. (In 2G there is no authentication, hence it is vulnerable to such an attack. 4G, 5G has defense against IMSI catchers)

→ Analogy: Peeking into your lunchbox without eating anything.

Attacks – Passive & Active

Attacks are usually divided into two broad types — passive attacks and active attacks.

Active Attacks – disruptive actions

- Masquerade: Pretending to be someone else.
- Replay: Capturing and resending login messages.
- Modification: Changing transaction values.
- Denial of Service: Flooding servers until they crash.

→ Analogy: Stealing your sandwich and replacing it with broccoli.

.

Modern Attack Patterns

Command-and-Control (C2) Communication

o Once malware infects a system, it usually calls back to a C2 server — a hidden server run by the attacker.

o This channel lets the attacker issue commands, exfiltrate data, and even update malware.

Example: In ransomware attacks, infected machines often communicate with a C2 infrastructure before encrypting files.

Real-world case: The SolarWinds hack (2020) — attackers used trojanized software updates, and the malware communicated silently with attacker-controlled servers.

→ **Analogy**: Imagine a spy inside your castle who secretly sends daily reports to the enemy commander. The spy can also receive new orders — like when to sabotage or steal.

Modern Attack Patterns

Advanced Persistent Threats (APTs)

o APTs are long-term, stealthy campaigns usually carried out by nation-states or organized groups.

o They don't just hack once and leave. They infiltrate, stay hidden for months or years, and slowly exfiltrate valuable information.

o Targets: Governments, defense contractors, critical infrastructure, banks.

Example: APT29 (Cozy Bear) targeting governments, APT41 targeting telecoms and healthcare.

This is not a teenager in a basement — this is highly funded, highly skilled, patient adversaries.

→ **Analogy:** Think of a termite infestation in a wooden house. You don't notice immediately. They quietly eat away at the foundation for months until one day, the structure collapses.

Modern Attack Patterns

OWASP Top Threats (Application-Level Attacks)

- o Most organizations today rely on web applications. Attackers target them using techniques documented in the OWASP Top 10.
- o SQL Injection: Inserting malicious code into a database query to steal or corrupt data.
- o Cross-Site Scripting (XSS): Injecting malicious scripts into websites to steal cookies or hijack sessions.
- o Broken Authentication: Weak login mechanisms that allow account takeover.
- o Insecure Deserialization / API Attacks: Manipulating poorly designed APIs to execute malicious code.

Example: Equifax breach (2017) → due to an unpatched web application vulnerability in Apache.

→ **Analogy:** Imagine a castle where the front gate is well-guarded, but a tiny hole in the side wall lets the enemy slip in unnoticed. That’s a vulnerable web app in modern infrastructure.

Case Studies

GitHub DDoS attack (2018): Largest at the time, 1.35 Tbps flood. → Availability failure.

Latest Cloudflare DDoS attack (2025): The most recent record-breaking DDoS attack was a 7.3 terabits per second (Tbps) event in mid-May 2025, which Cloudflare mitigated against an unnamed hosting provider. This multi-vector attack, consisting primarily of UDP floods, delivered 37.4 terabytes of data in just 45 seconds.

→ Availability failure.

Case Studies

Equifax breach (2017): Exploited OWASP-style vulnerability. The Equifax data breach of 2017 exposed the personal information of approximately 147 million people, including names, addresses, birth dates, Social Security Numbers, and driver's license numbers, and in some cases, credit card numbers. The breach occurred due to Equifax's failure to patch a known vulnerability in the Apache web application, which allowed hackers to infiltrate the system in mid-May 2017. They failed to detect on time as well.

→ Confidentiality failure.

Bangladesh Bank heist (2016): Manipulated SWIFT messages. Millions of reserves lost. → Integrity failure.

SolarWinds (2020): Classic supply-chain + C2 + APT example.

Step 1: Trusted Vendor Compromised Hackers broke into SolarWinds, a widely used IT software provider.

Step 2: Malicious Update Released. A software update containing hidden malware was sent to ~18,000 customers.

Step 3: Silent Infiltration Begins. Organizations installed the update, unknowingly allowing hackers inside.

Step 4: Remote Access Established. Malware connected back to attackers, giving them control over systems.

Step 5: Targeted Espionage. Hackers focused on high-value targets like Pentagon and homeland security (yes!)

Step 6: Long-Term Undetected Access. Attackers stayed hidden for months, stealing sensitive data.

Step 7: Discovery & Response. The breach was discovered, triggering investigations and emergency actions.

Step 8: Global Impact Realized. Hundreds of top organizations affected; trust in software supply chains shaken.

→ Multi-stage failure across CIA.

Wrap-Up

- Cybersecurity Journey
- InfoSec, NetSec, Cybersecurity clarified
- CIA Triad foundation
- Attacks: Passive vs Active
- Modern threats

Bridge to Next Class

Here’s the question that should be burning in your mind: If attackers have so many tricks, how do we fight back?

That is where security services and mechanisms come in. Next class, we move from the problems to the solutions. We’ll learn how to defend against these attacks. We’ll talk about security services and mechanisms — the actual tools in our toolkit, how encryption, authentication, digital signatures, and access control protect against the attacks we discussed today.

- **Services are like the goals:** ensuring confidentiality, integrity, authentication, access control, nonrepudiation, and availability.
- **Mechanisms are the tools:** to achieve those goals; encryption, hashing, digital signatures, firewalls, and authentication protocols.

Think of it this way: If the CIA triad tells us what we must protect, then security services and mechanisms tell us how we protect it.