



MONDAY – DAY 1

The Cybersecurity Landscape & Career Paths

Why it matters, and where you fit in

Facilitator Teaching Guide – Cybersecurity Track, Week 1
Prepared for Kelechi Nkwocha, Cybersecurity Track Facilitator

1. Learning Objectives

By the end of this session, students should be able to explain what cybersecurity is and why it has become a board-level priority, describe the main categories of cyber risk facing organizations today, and identify which entry-level career path in security best matches their own interests and strengths.

2. What Is Cybersecurity, Really?

Cybersecurity is the practice of protecting systems, networks, devices, and data from unauthorized access, disruption, or damage. But framed that way it sounds abstract. In practice, cybersecurity is a people problem wearing a technology costume: most breaches happen because a person clicked something, misconfigured something, or reused a password, not because an attacker broke unbreakable math.

Teaching tip: open the class by asking students to name a data breach they have heard of. Almost every hand will go up. Use that to make the point that this is not a niche topic; it is now a core function of every serious organization, from a five-person startup to a national government.

3. Why It Matters: The Scale of the Problem

- Cybercrime is now one of the largest illicit economies in the world, with global damages estimated in the trillions of dollars annually, rivaling the GDP of major nations.
- The frequency and sophistication of attacks continues to climb as more of daily life, banking, healthcare, government services, and critical infrastructure, moves online.
- Small and medium businesses are increasingly targeted precisely because they often have weaker defenses than large enterprises, making this a relevant concern in Nigeria and across Africa, not just for multinational firms.
- Skilled cybersecurity professionals remain in chronic short supply worldwide, which is precisely what makes this such a strong career track for students starting today.

4. Core Categories of Threats (Preview)

Wednesday's session goes deep on threat types, but it helps to preview the map today so students see where the pieces fit. Broadly, threats fall into a few buckets: malware (malicious software such as viruses, ransomware, and spyware), social engineering (manipulating people rather than machines, such as phishing), network-based attacks (intercepting or disrupting traffic), and insider threats (harm caused by someone who already has legitimate access).

5. Cybersecurity Career Paths

One of the most common misconceptions is that cybersecurity means one job: 'hacker.' In reality it is a wide field with distinct specializations. Walk students through each of these, since one of today's goals is helping them see themselves in this field.

Security Operations Center (SOC) Analyst

The most common entry point into the field. SOC analysts monitor security alerts, investigate suspicious activity, and escalate real incidents. This role is covered in depth in Week 5 of this track. It is the classic first job for

career-changers because it builds broad exposure fast.

Penetration Tester / Ethical Hacker

Simulates real-world attacks against an organization's own systems, with permission, to find weaknesses before criminals do. Pays well (commonly in the range of a hundred thousand to over two hundred thousand US dollars annually in mature markets) but usually requires a few years of foundational experience first, often starting in a SOC.

Governance, Risk & Compliance (GRC)

A strong entry path for students coming from a business, legal, or administrative background rather than a deeply technical one. GRC professionals write security policy, manage regulatory compliance, and assess organizational risk.

Identity & Access Management (IAM) / Network & Cloud Security

More technical specializations, suited to students who enjoy systems and infrastructure work. These roles control who can access what, and secure the underlying networks and cloud platforms an organization runs on.

Threat Intelligence Analyst

A strong fit for students who enjoy research and writing. This role tracks attacker groups, campaigns, and emerging techniques, and turns that research into guidance the rest of the security team can act on.

Facilitator note

A realistic route through this field for most beginners is: IT support or help-desk experience, then SOC Analyst Tier 1, then a specialization (penetration testing, cloud security, GRC, or threat intel) after two to three years. Encourage students to see the SOC analyst role, which this track builds toward, as a genuine launchpad rather than a lesser first step.

6. Class Discussion Prompts

- Which of the five career paths just described sounds most interesting to you right now, and why?
- Think of an organization you interact with often, a bank, a telecom provider, a hospital. What would happen to you personally if that organization suffered a major breach?
- Cybersecurity is often called a people problem as much as a technology problem. Do you agree, based on what we covered today?

7. Key Terms Introduced Today

- Cybersecurity — the practice of protecting systems, networks, and data from unauthorized access or harm.
- Threat — any potential cause of an unwanted incident that could harm a system or organization.
- SOC (Security Operations Center) — a centralized team that monitors and responds to security incidents.
- GRC — Governance, Risk, and Compliance; the policy and oversight side of security.

8. Looking Ahead

Tomorrow's session introduces the CIA triad, confidentiality, integrity, and availability, the foundational model that underlies almost every security decision covered for the rest of this course. Encourage students to keep today's threat categories in mind, since Tuesday will show how the CIA triad is really a framework for evaluating exactly those threats.