INTRODUCTION TO CYBER SECURITY

Cyber threats to public & Motivation of Cyber Attacks

TITUS G. GOODING

M.Sc. Software Engineering/Quality Assurance

Research Area: Cybersecurity and Data Science

I am the Executive Director of Code Brain Liberia, Training and Capacity development Director at Liberia cyber Crime and Mitigation Agency (LCCMPA), Consultant at both Technopreneur Liberia and Pro-tech Inc. I have written two publication on cybersecurity in the I. J. Computer Network and Information Security, 2019, 12, 40-48 (http://www.mecs-press.org/.../ijcnis.../IJCNIS-V11-N12-5.pdf.)

Course Outline

LECTURE ONE.

INTRODUCTION TO CYBER-SECURITY

LECTURE TWO.

CYBER THREATS TO PUBLIC

LECTURE THREE.

MOTIVATION TO CYBER ATTACKS

LECTURE ONE

We will cover following:

- What is cybersecurity
- CIA
- Cybersecurity Environment

Cybersecurity

- The connected electronic information network has become an integral part of our daily lives. All types of organizations, such as medical, financial, and education institutions, use this network to operate effectively. They utilize the network by collecting, processing, storing, and sharing vast amounts of digital information. As more digital information is gathered and shared, the protection of this information is becoming even more vital to our national security and economic stability.

Cybersecurity

- Cybersecurity is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm. On a personal level, you need to safeguard your identity, your data, and your computing devices. At the corporate level, it is everyone's responsibility to protect the organization's reputation, data, and customers. At the state level, national security, and the safety and well-being of the citizens are at stake.

Your Online and Offline Identity

As more time is spent online, your identity, both online and offline, can affect your life. Your offline identity is the person who your friends and family interact with on a daily basis at home, at school, or work. They know your personal information, such as your name, age, or where you live. Your online identity is who you are in cyberspace. Your online identity is how you present yourself to others online. This online identity should only reveal a limited amount of information about you.

Your Online and Offline Identity cont…

You should take care when choosing a username or alias for your online identity. The username should not include any personal information. It should be something appropriate and respectful. This username should not lead strangers to think you are an easy target for cybercrimes or unwanted attention.

CIA

The main purpose of cybersecurity is to ensure Confidentiality, Integrity and Availability (CIA) of data and services. The CIA is a model that is used to secure information. The CIA is essential in cybersecurity as it provides important security considerations to safeguard and protect critical information. We will understand how CIA enhances our security.

Confidentiality

Confidentiality refers to efforts to keep data private or secret.

Confidentiality ensures that information is accessed only by authorized personnel.

For example, access to an Institution network/ data should be granted to only authorized user/staff.

Unauthorized personnel should not be allowed to access any sensitive data as this could lead to privacy issues and data breaches.

A data breach is a security incident that exposes confidential or protected information to the public or to unauthorized parties.

Integrity

Integrity is about ensuring that data has not been tampered with. Therefore, integrity prevents

unauthorized modification or deletion of data. Only authorized personnel should be allowed to make

changes or delete data. It ensures that the data is correct, authentic, and reliable. Data must be protected

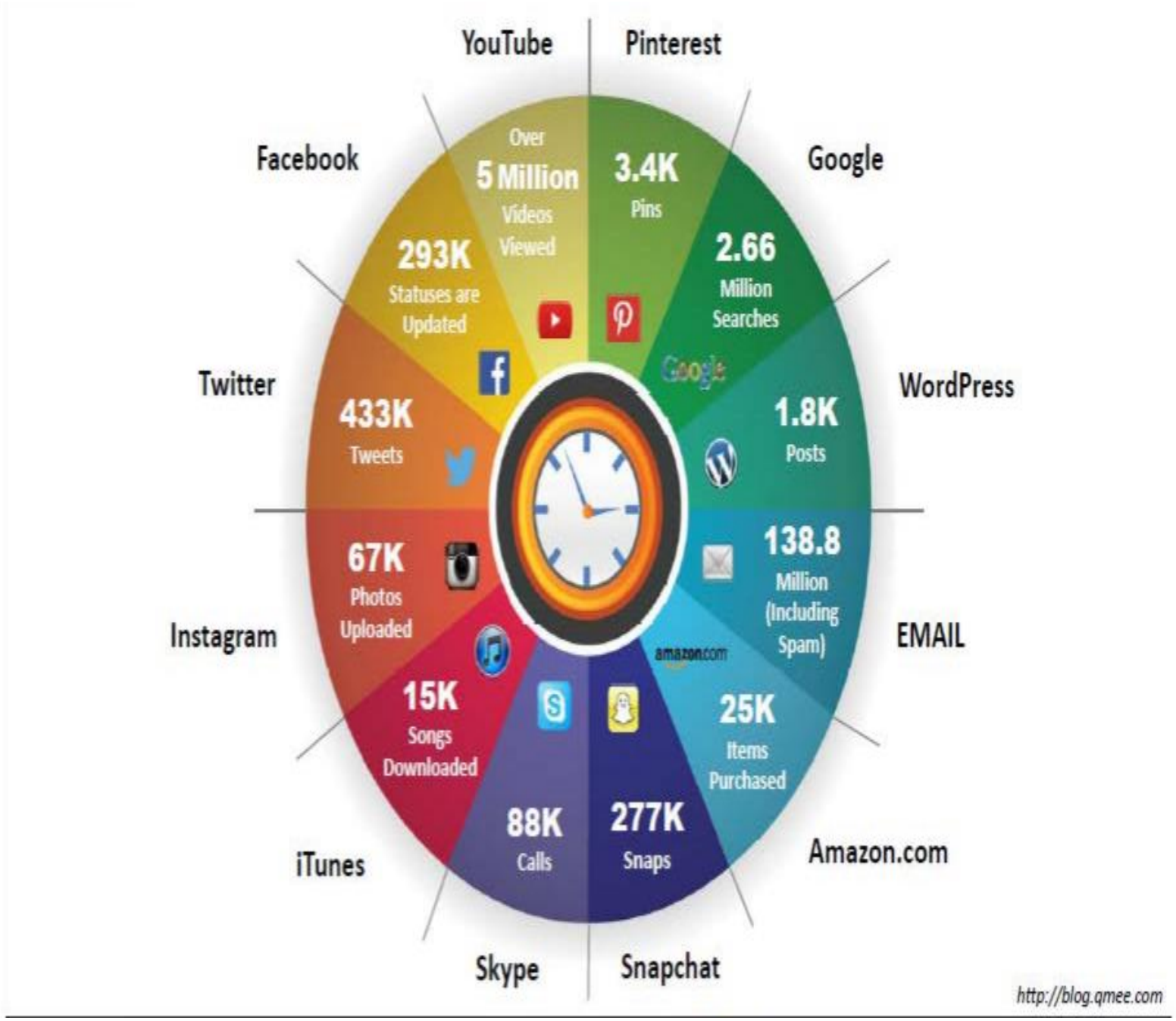
while in use, in transit, and when stored.

Availability

Availability refers to the guarantee of reliable and timely access to information and services by authorized

people. This ensures that authorized personnel can access networks, systems, applications and

information whenever needed



Cybersecurity Environment

Cybersecurity environment refers to the Cyberspace

The Cyberspace is a concept describing a widespread, interconnected digital technology

www.internet Live statics.com

Internet of Things and Big Data

With the emergence of the Internet of Things (IoT), there is a lot more data to manage and secure.

IoT is a large network of physical objects,

such as sensors and equipment that extend beyond the traditional computer network.

All these connections, plus the fact that we have expanded storage capacity and storage services through the cloud and virtualization, lead to the exponential growth of data.

This data has created a new area of interest in technology and business called “Big Data". With the velocity, volume, and variety of data generated by the IoT and the daily operations of business, the confidentiality, integrity and availability of this data is vital to the survival of the organization.

Lecture two

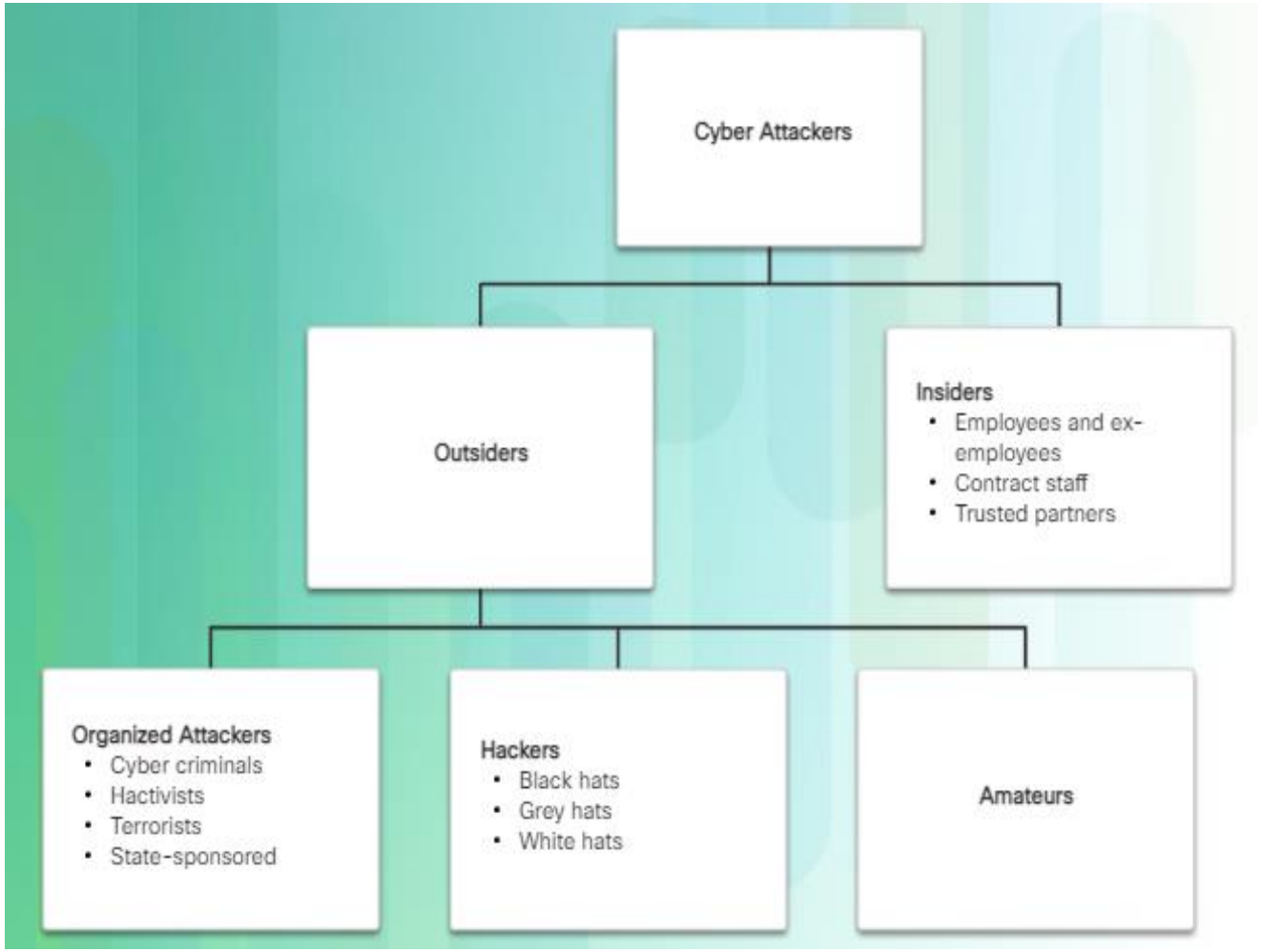
Threats

Types of Threats

Threats

- the Oxford Dictionary definition of cyber threat is a little lacking: “the possibility of a malicious attempt to damage or disrupt a computer network or system.”

- This definition is incomplete without including the attempt to access files and infiltrate or steal data.
- In this definition, the threat is defined as a possibility. However,
- in the cybersecurity community, the threat is more closely identified with the actor
- or adversary attempting to gain access to a system. Or a threat might be identified by
- the damage being done, what is being stolen or the tactics, Techniques and Procedures (TTP) being used.



Types of Threats

- Today's cybercrime landscape is diverse. Cyber threats typically consist of one
- or more of the following types of attacks: Advanced Persistent Threats, Phishing, Trojans, Botnets, Ransomware, Distributed Denial of Service (DDoS), Wiper Attacks, Intellectual Property Theft, Theft of Money, Data Manipulation, Data Destruction, Spyware/Malware, Man in the Middle (MITM), Drive-By Downloads, Advertising, Rogue Software, Unpatched Software.

- Threats can be categorize in two simple types:
- Exterior Threats/Outsider
- Interior or Insider Threats

Lecture Three

MOTIVATION TO CYBER ATTACKS

MOTIVATION

- In order to effectively against cyberattacks, it is important to understand the purposes and motivation behind all the attacks. Even though the methods and purposes of cyberattacks are varied, the major motivations can be categorized into 6 types as shown below: **Political Or Social Point, Radical Hackerism, Financial Gain, Intellectual Challenge, Business Competition, Cyberwarfare.**

Political Or Social Point, Radical Hackerism.

- **Political Or Social Point:** Hackers can attack for expressing their criticism of everything from governments, politicians, society, big brand companies, and current affairs. They tend to attack their targets, such as crashing their website, when they disagree with them
- **Radical Hackerism:** This group of people is usually formed by boring teens who seek a surge in adrenaline or try to vent their anger or frustration with institutions (such as schools) or with people they believe to be wrong. In addition, some people are just seeking attention and respect from peers.

Financial Gain and Intellectual Challenge

- **Financial Gain :** This is the most likely reason an organization gets attacked. Nearly three-quarters of cyberattacks are essentially for financial gains, such as stealing money directly from financial accounts, stealing credit card information, causing data breaches, demanding ransom, and etc. Many companies went offline after refusing to pay the ransom and succumb to the threat of blackmailers.
- **Intellectual Challenge :** Similiar to radical hackerism, this group of people commit cyberattacks for seeking attention and respect from peers through
- challenging network security. This type of hacker plays to the stereotype of the socially awkward loner who lives in a virtual world and turns to hack for
- both the intellectual challenge and the adrenaline rush of breaking into a network.

Business Competition, and Cyberwarfare.

- **Business Competition :** DDoS attacks are increasingly being used as a competitive business tool. Some of these attacks are designed to prevent competitors from participating in major events, while others target the complete shutdown of online businesses for months..
- **Cyberwarfare :**It is a war on the Internet and information flow. State-backed cyberattacks are being used as a means of suppressing government critics and internal opposition, as well as undermining important financial, health and infrastructure services in enemy countries. These attacks are backed by nation-states, which means they are well-funded and well-planned activities performed by tech-savvy professionals.

Course Progress

Lecture 1	Lecture 2	Lecture 3
INTRODUCTION TO CYBER-SECURITY	CYBER THREATS TO PUBLIC	MOTIVATION TO CYBER ATTACKS


THANK YOU!