HANDOUT 1 - WEEK 1 READING

Cybersecurity Fundamentals

CIS 350: AI for Cybersecurity - Smart Defense for the Digital Business

Colorado State University - Computer Information Systems

How to use this reading

This handout supports Week 1. Read it before and after class. It covers the vocabulary of security, the CIA triad, the main attack types, how organizations defend themselves, and why people are the most-targeted layer. The review questions at the end map directly to Quiz 1.

Estimated reading time: 20-25 minutes. No prior technical background needed.

1. Why Cybersecurity Matters for Business

Every modern organization runs on data and software, which means every organization is a target. Customer records, payments, intellectual property, and the systems that keep a business running are all valuable - and all at risk. A single security incident can mean lost money, legal penalties, damaged reputation, and downtime that stops the business cold.

The numbers make the point. Industry studies put the average cost of a data breach near 4.88 million dollars (IBM, 2024), and most incidents are not the work of criminal geniuses - they trace back to a missed update, a weak or reused password, or a single click on a convincing email.

Artificial intelligence has raised the stakes on both sides. Attackers use AI to write flawless phishing at scale and to generate malware that dodges simple filters. Defenders use AI to catch spam and fraud in milliseconds and to spot unusual behavior hidden in millions of events. Understanding both sides is exactly what this course is about - and it is a rare, valuable skill in any business role.

2. The Vocabulary of Security

Security has a small set of words you will use all semester. Learn these four first:

- Asset - anything worth protecting: data, money, systems, reputation, even people.
- Threat - anyone or anything that could cause harm (a hacker, malware, a natural disaster).
- Vulnerability - a weakness a threat can exploit (an unpatched server, a weak password).
- Risk - the chance that harm actually happens, combined with how bad it would be.

Threat actors: who is behind attacks?

- Cybercriminals - motivated by money through ransomware, fraud, and theft (most common).
- Hacktivists - pushing a political or social cause.
- Nation-states - well-funded groups focused on espionage or sabotage.
- Insiders - employees or partners, either malicious or simply careless.

Attack surface and risk

The attack surface is the sum of every possible way in: applications, devices, cloud services, vendors, and people. More devices and more remote work mean a larger surface to defend. Because we can never fix everything at once, security teams rank risks using a simple idea:

> **The risk equation**
>
> Risk = Threat x Vulnerability x Impact. The biggest risks (likely to happen AND painful if they do) are handled first. Organizations then choose how to treat each risk: Mitigate it with controls, Transfer it (for example, insurance), Avoid the risky activity, or knowingly Accept a small risk.

3. The CIA Triad

Almost every security decision aims to protect one of three goals, known together as the CIA triad.

Confidentiality - keep secrets secret

Only authorized people should be able to read sensitive data. Tools include encryption, access controls, the principle of least privilege, and strong passwords with multi-factor authentication. Confidentiality breaks when data leaks, a password is stolen, or an email goes to the wrong person.

Integrity - trust the data

Data and systems must be accurate and unaltered. Tools include hashing and checksums, change controls, digital signatures, and audit logs. Integrity breaks when an attacker edits bank balances, grades, or shipping records. If you cannot trust the data, you cannot trust any decision built on it.

Availability - there when you need it

Systems and data must be accessible to the right people on time. Tools include backups, redundancy, failover, and protection against denial-of-service attacks. Availability breaks when ransomware locks files or a flood of traffic knocks a site offline. A hospital that cannot reach patient records faces a safety emergency, not just an IT problem.

4. The Threat Landscape

Phishing - the number-one way in

Phishing is a fake message that looks legitimate and pushes you to act fast - to click a link, open an attachment, or hand over a password or payment. It is cheap, scalable, and now often AI-written, so the grammar is perfect. Variants include spear phishing (tailored to you), whaling (targeting executives), smishing (text messages), vishing (phone calls), and Business Email Compromise (fake invoices and urgent wire requests, which cause some of the largest financial losses of all).

Common red flags: urgency or threats, mismatched or look-alike links and senders, unexpected attachments, and requests for passwords, payment, or gift cards. The golden rule is to slow down and verify through a separate, trusted channel.

Malware and ransomware

Malware is any malicious software - viruses and worms (which can self-spread), trojans (hidden in something that looks safe), spyware, and botnets (armies of hijacked machines). Ransomware is malware that encrypts your files and demands payment; modern strains also steal a copy first and threaten to leak it. Recovery and downtime usually cost far more than the ransom, and paying is discouraged. Offline backups are the real defense.

Denial of service and insider threats

A Denial-of-Service (DoS) attack floods a service with junk traffic until real users cannot get in; a Distributed DoS (DDoS) uses a botnet to attack from thousands of machines at once. Insider threats come from people on the inside - malicious (theft or sabotage), negligent (a careless click or lost laptop), or compromised (an outsider using a real employee's stolen account).

5. Defending the Business: Defense in Depth

No single control is perfect, so organizations stack many independent layers - like slices of Swiss cheese, where the holes rarely line up. Defenses span people, process, and technology, and fall into three stages:

- Prevention - stop attacks before they land: training, multi-factor authentication, patching, least privilege, firewalls, and network segmentation.
- Detection - catch what slips through: logging, monitoring, intrusion detection, and AI-powered anomaly detection (the focus of several labs in this course).
- Response - limit the damage: contain the incident, eradicate the cause, recover, and learn from it.

Incident response in six steps

Prepare, Identify, Contain, Eradicate, Recover, and Learn. The goal is not to never get hit - it is to detect quickly, contain the damage, recover, and come back stronger. Teams that practice their playbook lose far less.

6. The Human Factor

Roughly two out of three breaches involve a human element (Verizon DBIR). People can be rushed, tricked, or tired, so fooling a person is often easier than breaking strong encryption - and one click can bypass every firewall. Social engineering is the art of manipulating people, and it exploits predictable mental shortcuts:

- Urgency - 'act now or lose access' shuts down careful thinking.
- Authority - pretending to be the CEO, IT, or police.
- Scarcity and reward - 'only 2 left' or 'you won a prize'.
- Trust and social proof - impersonating a coworker or claiming 'everyone already did this'.

The good news: trained, alert people are also the best early-warning system. You are a security control. Pause on urgency, verify through a second channel, never share passwords or one-time codes, and report anything suspicious. A no-blame culture - where it is safe to ask 'is this real?' - stops attacks early.

7. AI on Both Sides

AI is now woven through both attack and defense. Attackers use it to personalize phishing, generate malware variants, clone voices and faces (deepfakes), and automate the search for weak systems. Defenders use it to filter spam and fraud, detect unusual logins and traffic, triage floods of alerts, and prioritize the risks that matter most. Over the semester you will build beginner-friendly versions of these defensive tools yourself - no heavy math required.

Key Terms

- CIA triad - Confidentiality, Integrity, Availability.
- Asset / Threat / Vulnerability / Risk - what we protect, what could harm it, the weakness, and the chance plus impact of harm.
- Phishing / spear phishing / BEC - deceptive messages, targeted versions, and fake payment requests.
- Malware / ransomware / DDoS - malicious software, file-locking extortion, and traffic floods.

- Defense in depth - layered prevention, detection, and response.
- Social engineering - manipulating people rather than machines.
- MFA - multi-factor authentication; a stolen password alone is not enough to log in.

Review Questions (self-check for Quiz 1)

- What do the three letters of the CIA triad stand for, with one example of each?
- Give an example of a threat, a vulnerability, and the resulting risk.
- Name three common attack types and one defense for each.
- What are the three stages of defense in depth?
- Why are people often the most-targeted layer, and what habits reduce that risk?
- Give one way attackers use AI and one way defenders use AI.

Bring your questions to class - and remember that AI tools are not permitted on quizzes and labs in this course.