Intro to Cybersecurity

1.1.1 – Intro to Security Concepts

GALANTECH with GARDEN STATE CYBER

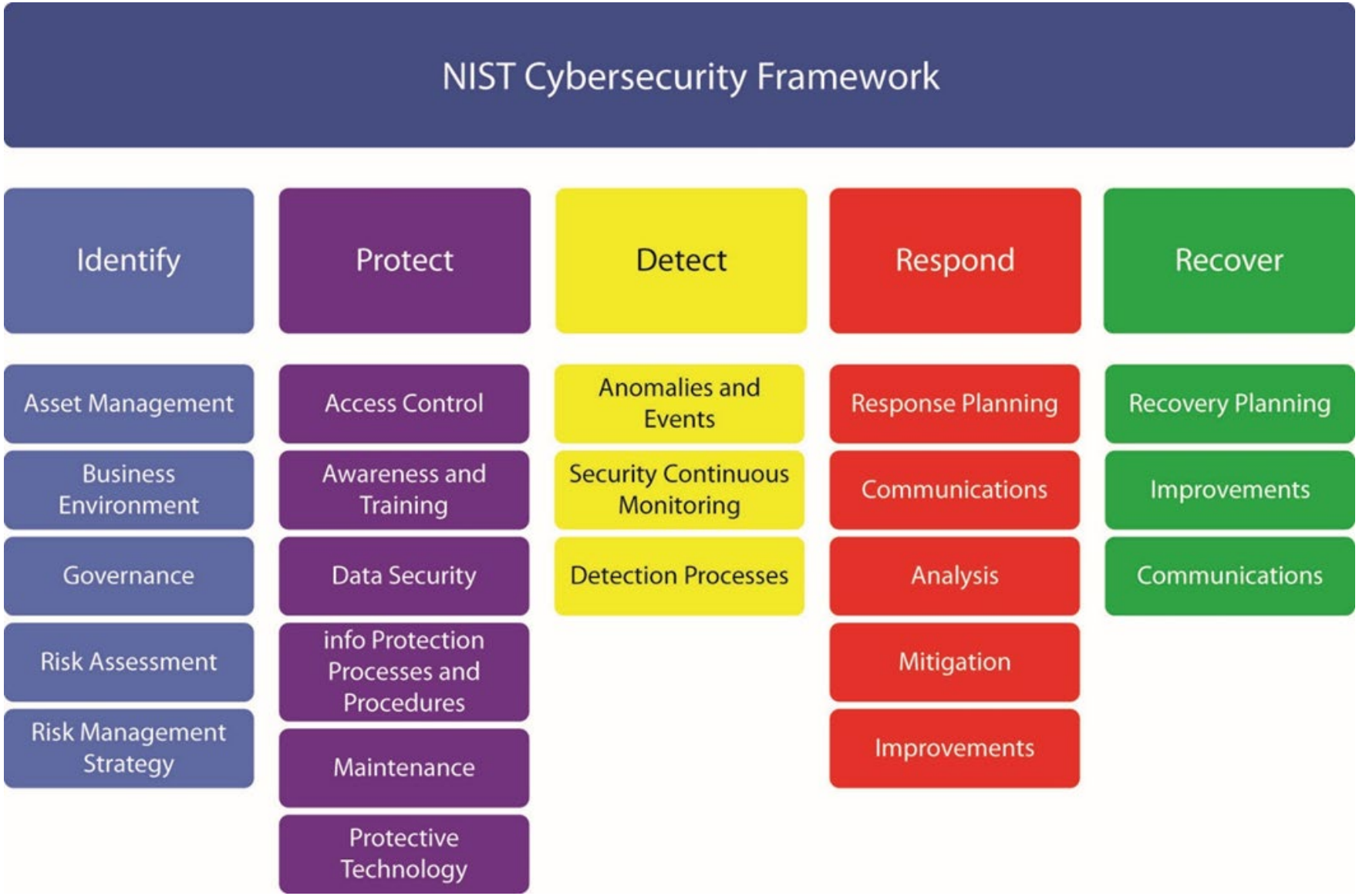
CYBER.ORG

Model of Computer Security

Protection = Prevention + (Detection + Response)

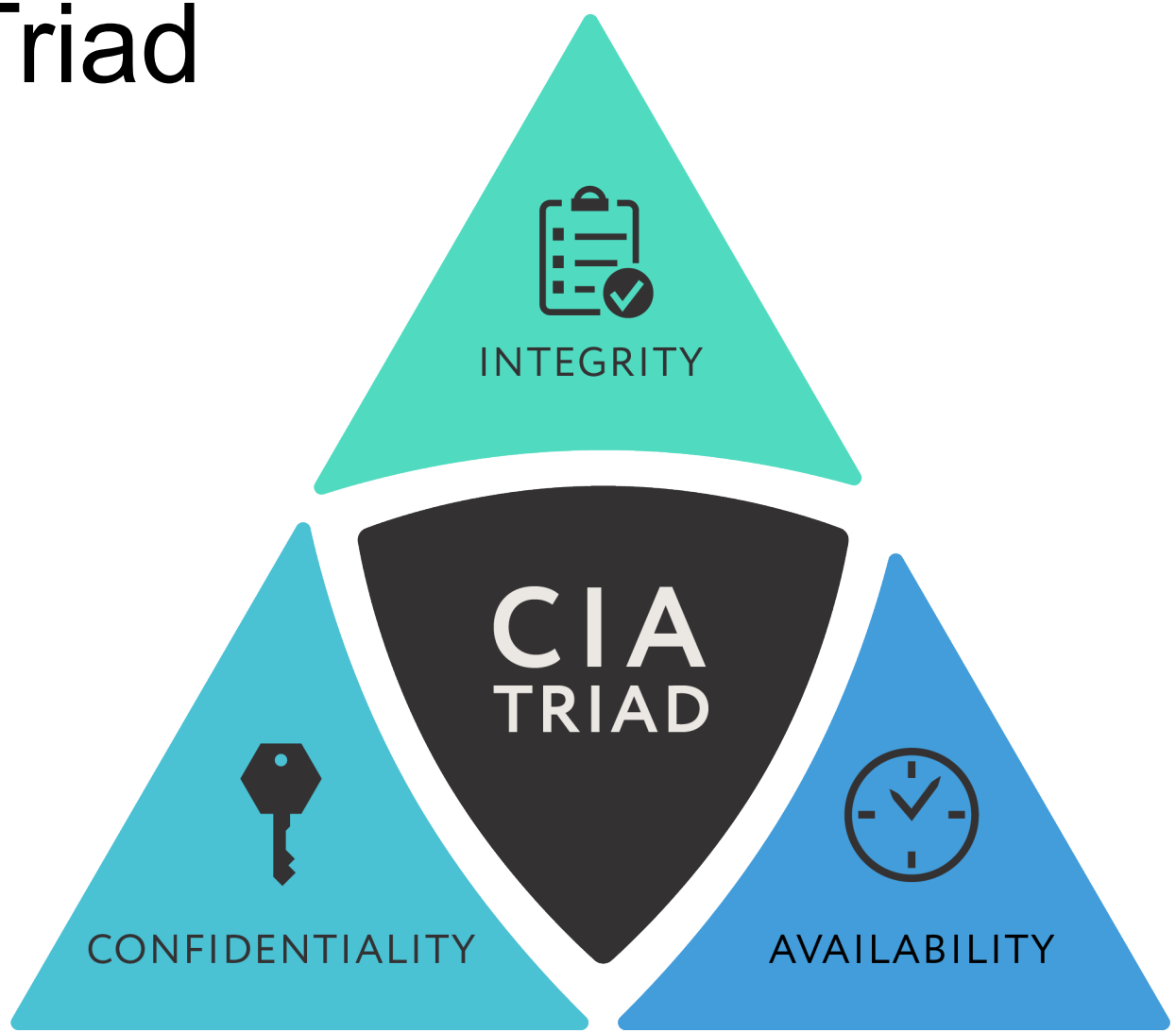
- **Protection** – What the goal is.
- **Prevention** – What you can do ahead of time.
- **Detection** – What you can do while the system is running to determine if something is wrong.
- **Response** – When something wrong is detected what you can do to fix the problem.

- Every security technique falls into at least one of the three elements of this equation



Source: https://www.nist.gov/cyberframework

The CIA Triad



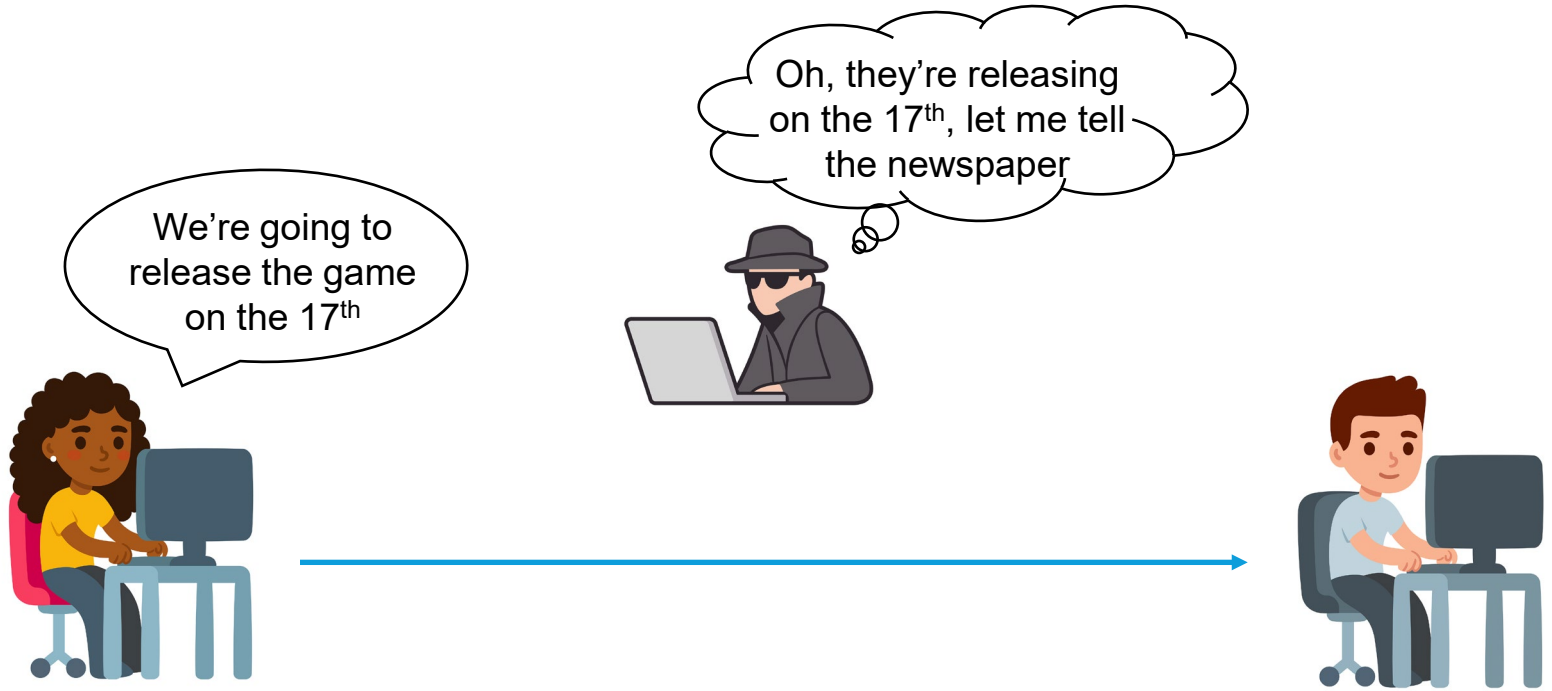
C I A = Goal of Network Security

Data (aka information) is an Asset. The goal of cybersecurity is to maintain…

Confidentiality	Data is not revealed
Integrity	Data is intact – not modified or corrupted
Availability	Data is accessible to allowed users

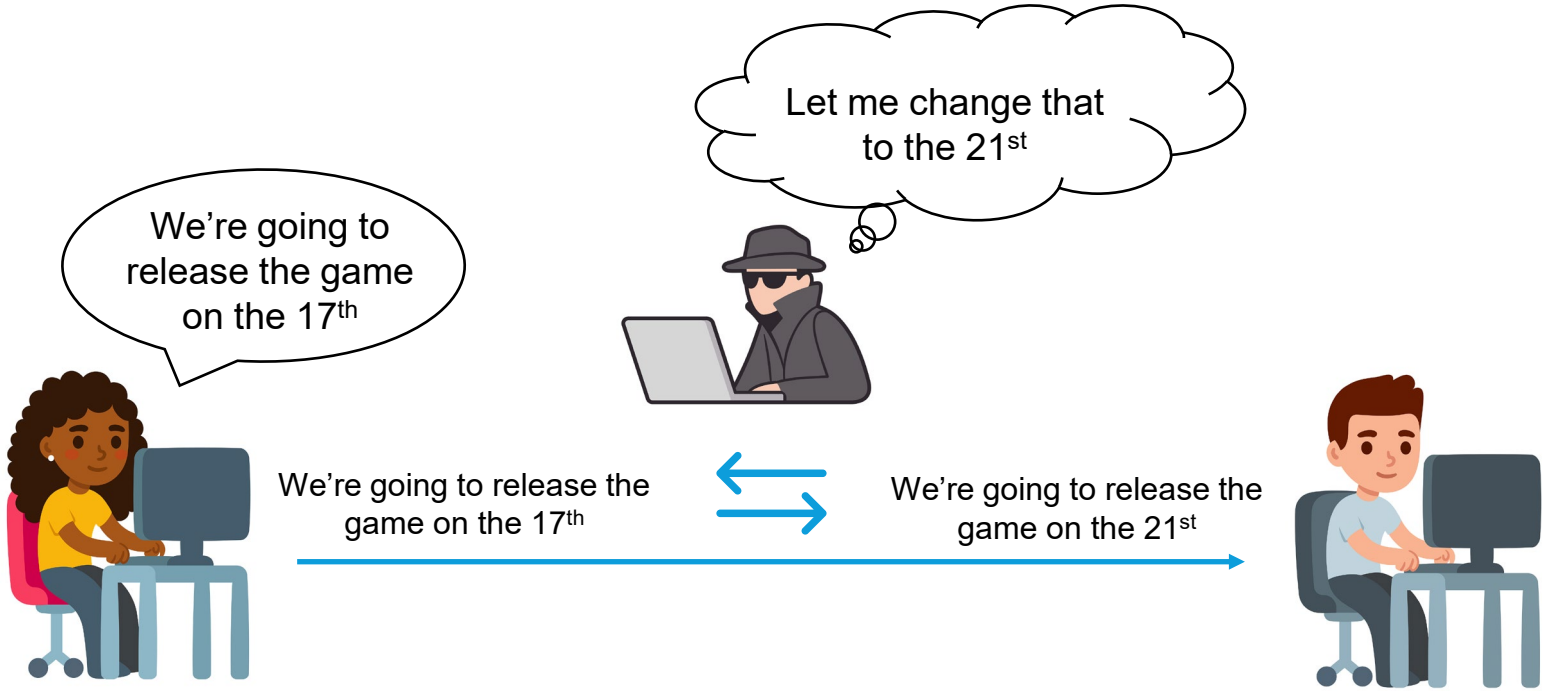
Confidentiality

Protection against unauthorized access



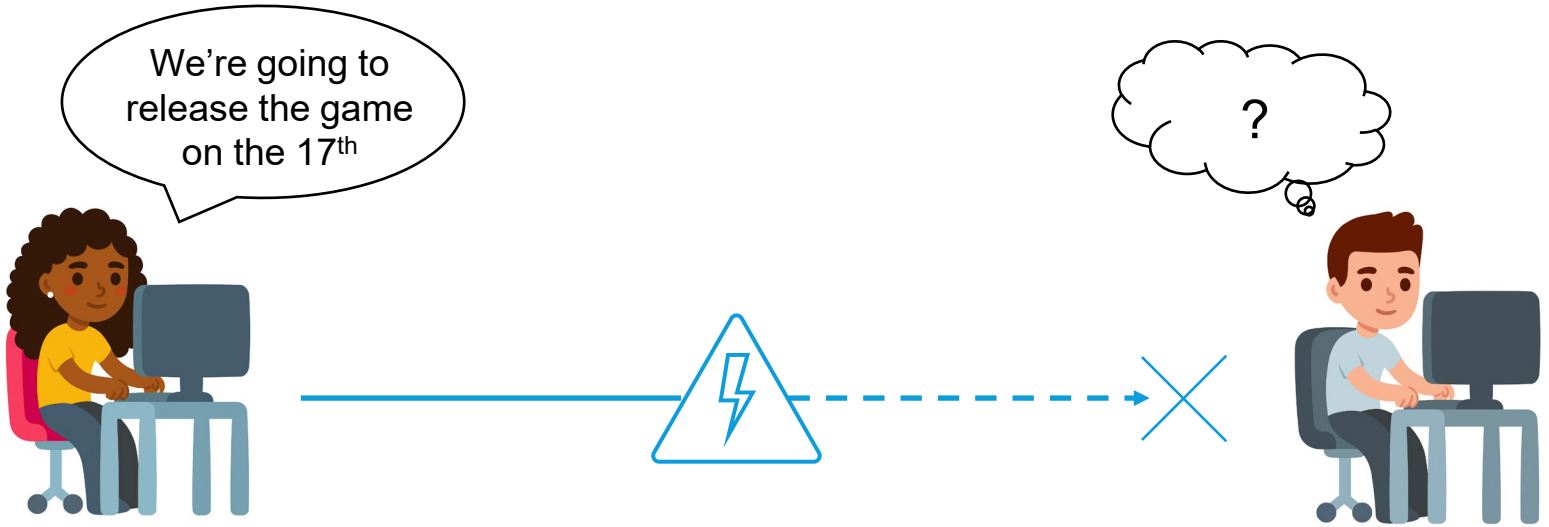
Integrity

Protection against unauthorized modification



Availability

Protection against denial of service



Intro to Cybersecurity

Activity – Understanding the CIA Triad

GALANTECH with GARDEN STATE CYBER

CYBER.ORG

Data “states”

To protect the CIA of data, we need to know what *“state”* the data is in and then we can apply the right cybersecurity tool.

- **Data at Rest** = *storage* → information is at rest; usually files, databases, etc stored on hard drives, USB drives, memory, DVDs

- **Data in Transit** = *transmission* → being moved from one system to another or file sharing on a LAN or transfer on the Internet, etc.

- **Data in Use** = *processing* → file creation by user, data used in an application, being processed or placed in memory, etc.

Breach of CIA examples

Loss of Confidentiality
Stolen data that was made public

- NSA leaks of government data by Edward Snowden

NY Times 6/9/13 Credit:Glenn Greenwald/Laura Poitras/European Pressphoto Agency

Breach of CIA examples

Loss of Integrity → Data that was corrupted


Iran: Computer Malware Sabotaged Uranium Centrifuges

BY KIM ZETTER 11.29.10 4:18 PM

Follow @KimZetter

https://www.wired.com/2010/11/stuxnet-sabotage-centrifuges/

STUXNET worm – changed the code on the centrifuge machines in an Iranian nuclear facility so that they ran at too high a speed.

GALANTECH with GARDEN STATE CYBER

CYBER.ORG

Breach of CIA examples

Loss of Availability → Data is inaccessible

A common reason is a DDoS attack = *Distributed Denial of Service*

Mirai Botnet takes down website of cybersecurity reporter Brian Krebs– mad about an article he wrote, hackers infected more than 145,000 internet-attached devices like cameras and ordered them to flood Krebs' website with traffic. It was like getting hit with a massive firehose and the site crashed for 4 days.


BIZ & IT —

Record-breaking DDoS reportedly delivered by >145k hacked cameras

Once unthinkable, 1 terabit attacks may soon be the new normal.

DAN GOODIN - 9/28/2016, 8:50 PM

https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

GALANTECH with GARDEN STATE CYBER

CYBER.ORG

Intro to Cybersecurity

Activity – CIA Triad Card Game

GALANTECH with GARDEN STATE CYBER

CYBER.ORG