University of Colorado **Boulder**

CSCI 3403 INTRO TO CYBERSECURITY

Lecture: 2-1

Topic: Fundamentals

Presenter: Matt Niemiec

Announcements

- Next Tuesday, a security expert from Wal-Mart is giving a talk at CU
  - More details on next slide
  - Questions can be directed at Nolen Scaife
- Project 1 will be up after class
- Slides posted as class starts
- Shorter version up two days in advance (hopefully)

INDUSTRY LEADER FOCUSED ON BEST-IN-CLASS INFORMATION SECURITY PRACTICES, INNOVATION AND BUSINESS ENABLEMENT

JERRY GEISLER

Chief Information Security Officer

at

Walmart

TUESDAY, JANUARY 28

12:30-1:45 PM

ECCR 150

ANYBODY IS WELCOME!

Technology, Cybersecurity and Policy Program

UNIVERSITY OF COLORADO **BOULDER**

WALMART IS #1 ON FORBES FORTUNE 500 LIST

LEARN ABOUT THEIR AMAZING CYBERSECURITY PROGRAM

Types of Attacks

Active Attacks

- “An attempt to alter system resources or affect their operation”
- In general, easier to detect
- Threatens availability and/or integrity of data

Passive Attacks

- “An attempt to learn or make use of information from the system that does not affect system resources”
- Does not interfere with the system
- Generally harder to detect
- Threatens confidentiality of data

Categorize the Following

- Ransomware
- Monitoring pizzas delivered to the Pentagon
- DDoS
- Traffic sniffing
- Data breach
- Breaking encryption on private data

Inside vs. Outside Attack

- Inside attacks are at least as dangerous as outside attacks
- Inside attacks can happen from unsatisfied employees
- Inside attacks often non-intentional

Inside Attack

Mashable VIDEO ENTERTAINMENT CULTURE TECH SCIENCE SOCIAL GOOD SHOP MORE

Ex-Yahoo employee hacked 6,000 accounts for sexual images

Share on Facebook Share on Twitter +

Countermeasure

- A countermeasure is how you deal with a type of attack
- What countermeasure to use?
- Defend these types of attacks differently

Security Terminology

Asset

- Anything that is valuable to either the adversary or the victim
  - Hardware, software, data, networks
- Also called “system resource”

Vulnerability

- “Weakness... that could be exploited or triggered by a threat source”
- Basically, what we normally think of
- In general, very easy to detect

Threat

- Anything that is capable of exploiting a vulnerability
  - E.g. a ransomware software
- Can violate any of CIA of an asset
- Not threat actor or threat action

Attack

- “Any kind of malicious *activity* that attempts to collect, disrupt, deny, degrade, or destroy information system resources of the information itself”
- A threat in action

Risk

- A couple of ways to thing about risk
- In book: asset + vulnerability + threat
- In industry: loss x (probability of occurring)

Practice

- Consider a ransomware attack on your home network
- What is/are the...
  - Vulnerabilities
  - Assets
  - Threats
  - Risk
- Categorize the attack

Practice

- Consider the defense of a data storehouse
- What is/are the...
  - Vulnerabilities
  - Assets
  - Threats
  - Risk
- Categorize the attack

Threat Modeling

Who is Attacking?

- A foreign government (APT)
- A competing business
- Your roommate
- A curious attacker

What is their motivation?

- Curiosity
- Power (over foreign government)
- Business advantage
- Money

How Do We Defend...

- Your roommate who wants your money vs a large business who wants your money?

NIST Framework

The NIST Framework

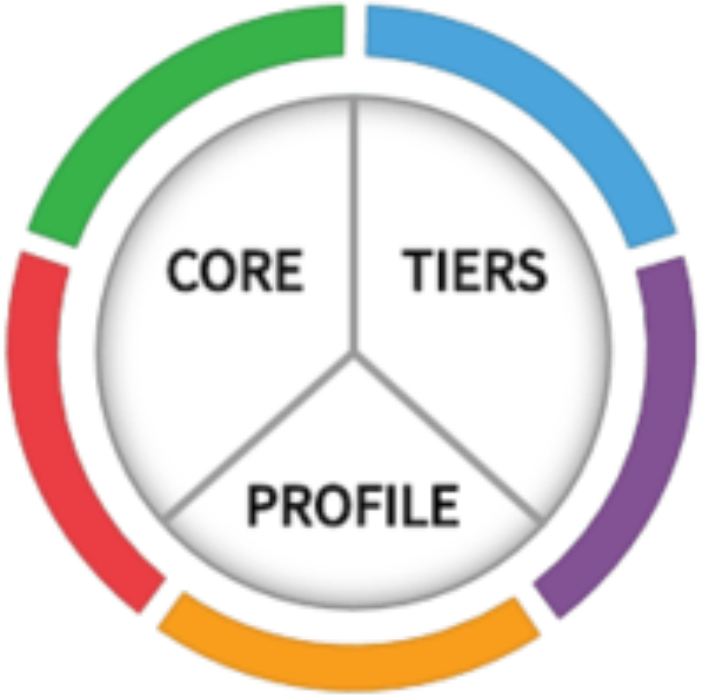
- A way of thinking about security
- Typically used by government
- One of many frameworks

What the NIST Framework ISN’T

- A solution to security :/
- Detailed
- Checklist security
- Static

The Three Parts

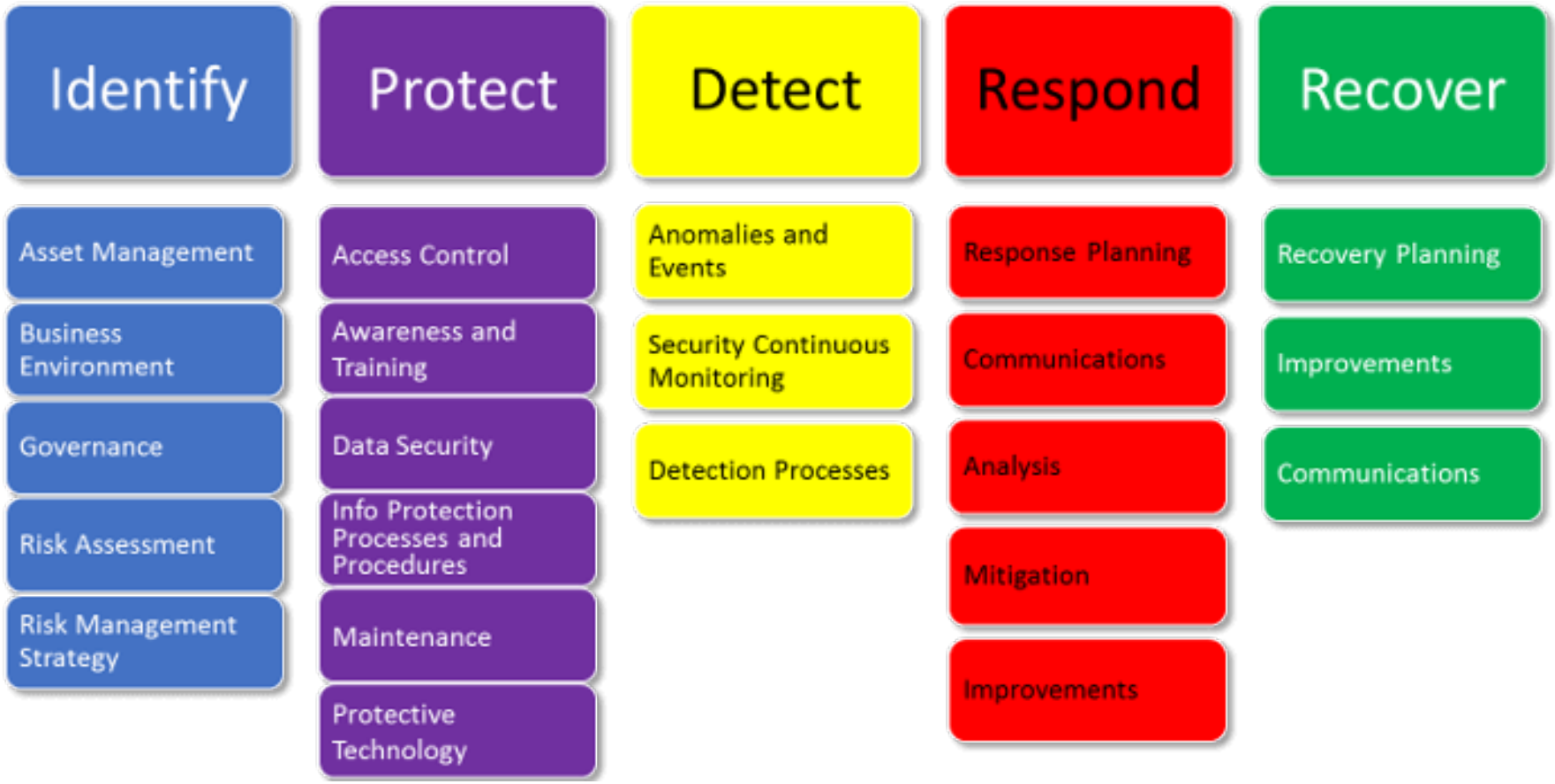
- Tiers is how mature your company's security is
- Profiles help your company grow into where it should be
- We only care about the Core



The Core

- Consists of five parts
- Each part is a different phase in a cyber attack
- Begins with Identify

NIST Cyber Security Framework

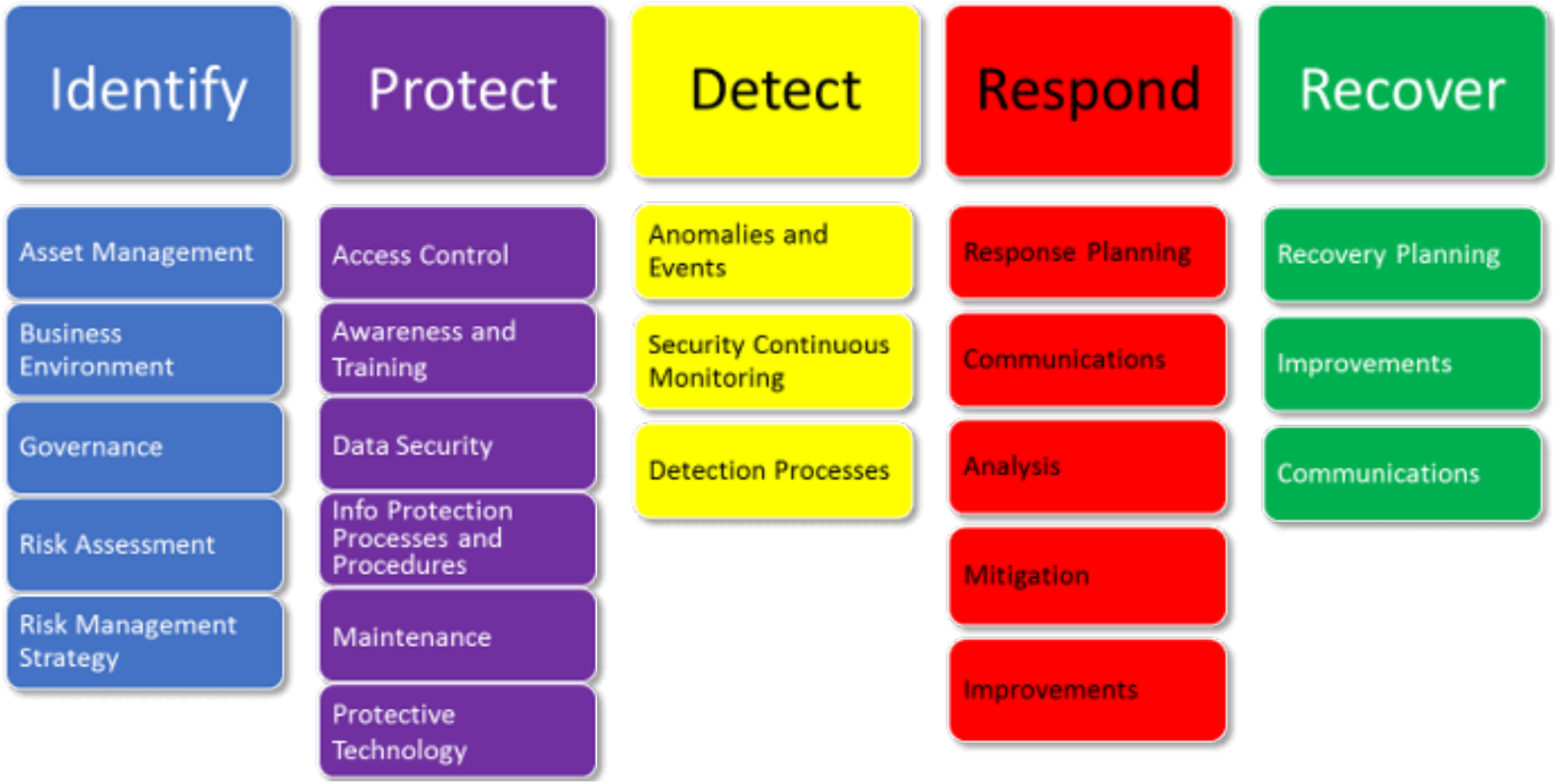


(Image source: Security Affairs.co)

Identify

- Your assets and resources
  - Includes time, personnel, ideas, etc.
- Network map
- Potential problems
- Prioritization

NIST Cyber Security Framework

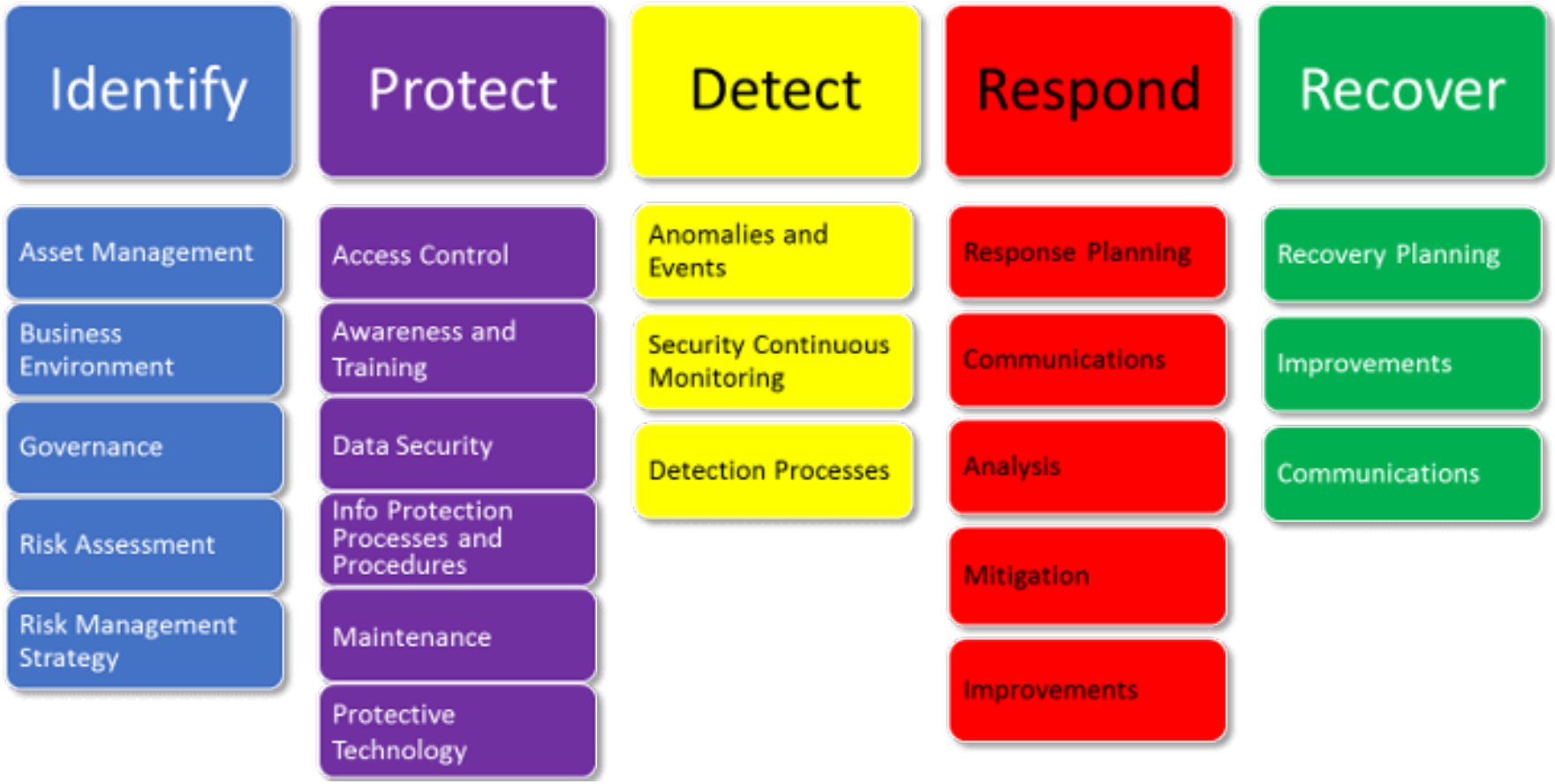


(Image source: Security Affairs.co)

Protect

- Don’t start here!
- Implement access control, authentication, encryption, honeypot, application whitelisting, etc.

NIST Cyber Security Framework

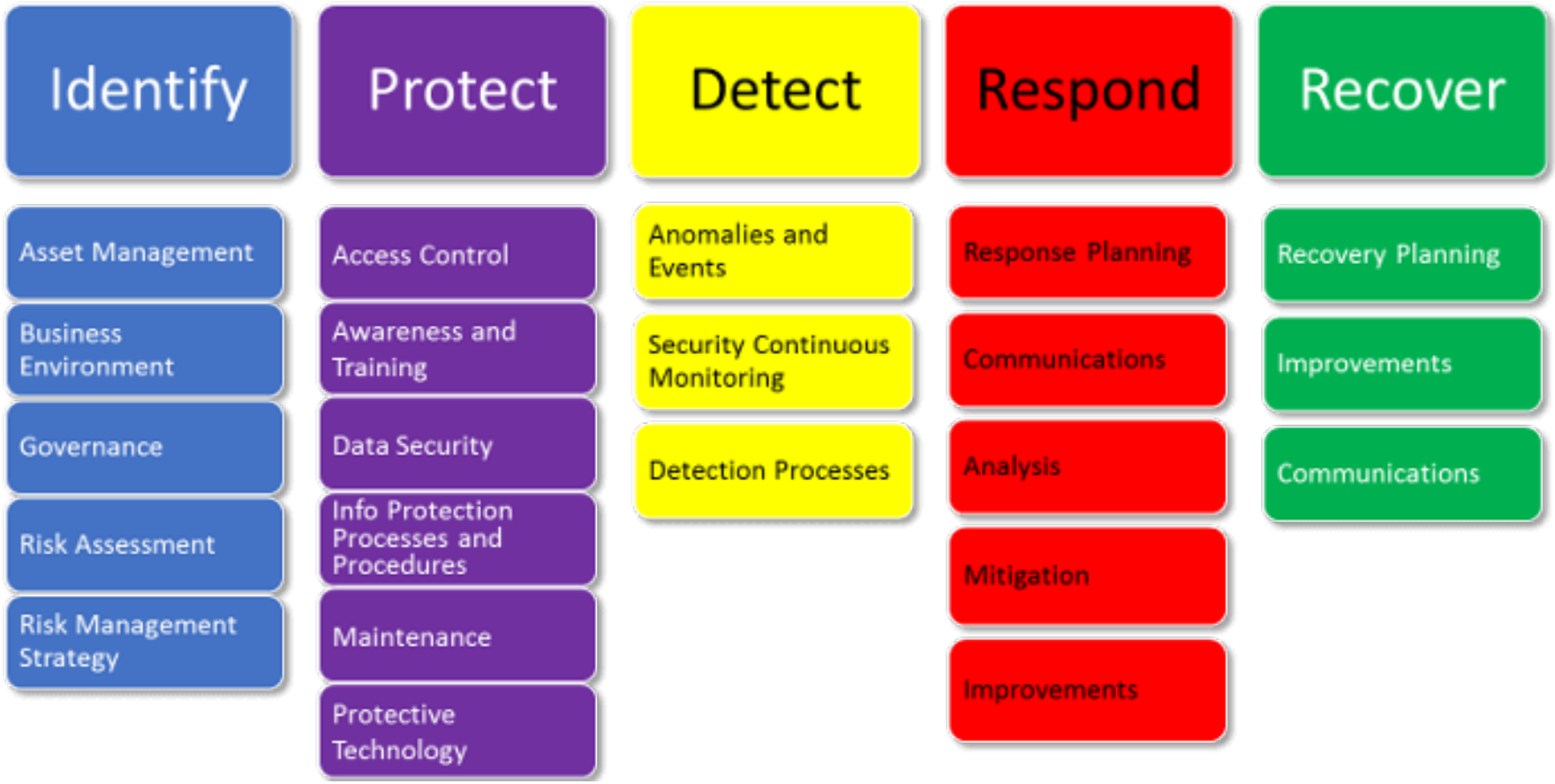


(Image source: Security Affairs.co)

Detect

- Know when you're being attacked
- Monitor network traffic, processes
- Collect data about the attack
- Anomaly vs. signature detection

NIST Cyber Security Framework

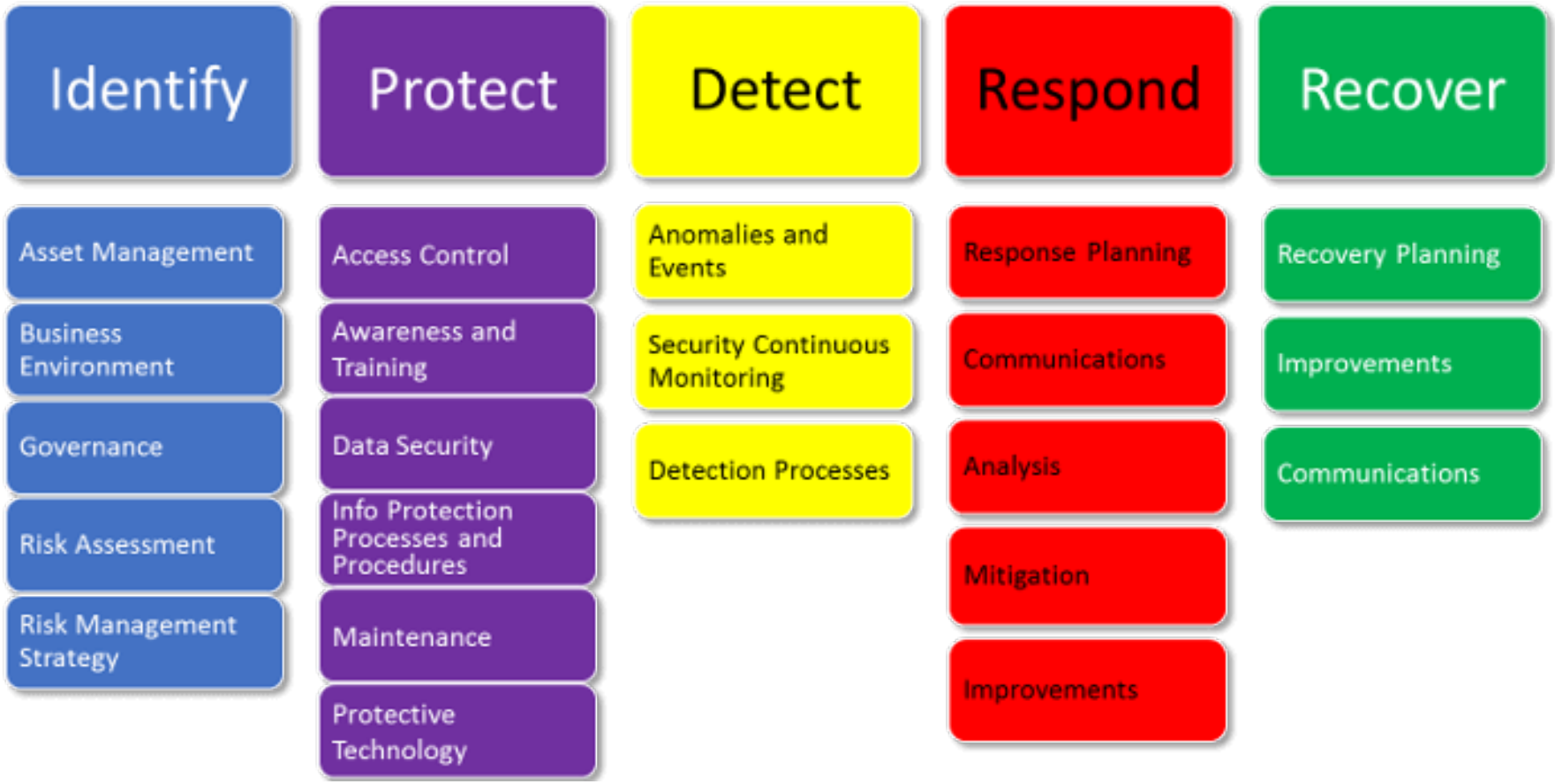


(Image source: Security Affairs.co)

Respond

- Step 1: Analyze the incident
- Step 2: Mitigate the incident
- Step 3: Improve the situation

NIST Cyber Security Framework



(Image source: Security Affairs.co)

Recover

- Do you have backups?
- Run an audit on the system?
- How can we further improve the system?

NIST In Short

- Gives us questions to start asking
- Need to think about
- Much broader than we typically think of

Reiteration on Fundamentals

Cybersecurity...

- Doesn’t have just one approach
- Requires knowing the adversary
- Can be thought of in different ways