Cybersecurity

CS 4950/5950
Homeland Security & Cybersecurity

Lesson 15
Cybersecurity

Rick White, Ph.D.
University of Colorado, Colorado Springs

1
Esc

1

"Cyber"

- **Prefix referring to computers and anything related to them.**
- Derived from "cybernetics", study of control systems.
  - Norbert Weiner, 1948
- Current usage tied to 1990s rise of Internet and common reference as "Cyberspace".
- Broad application makes it a multi-disciplinary area of study.

cy·ber
/ˈsībər/

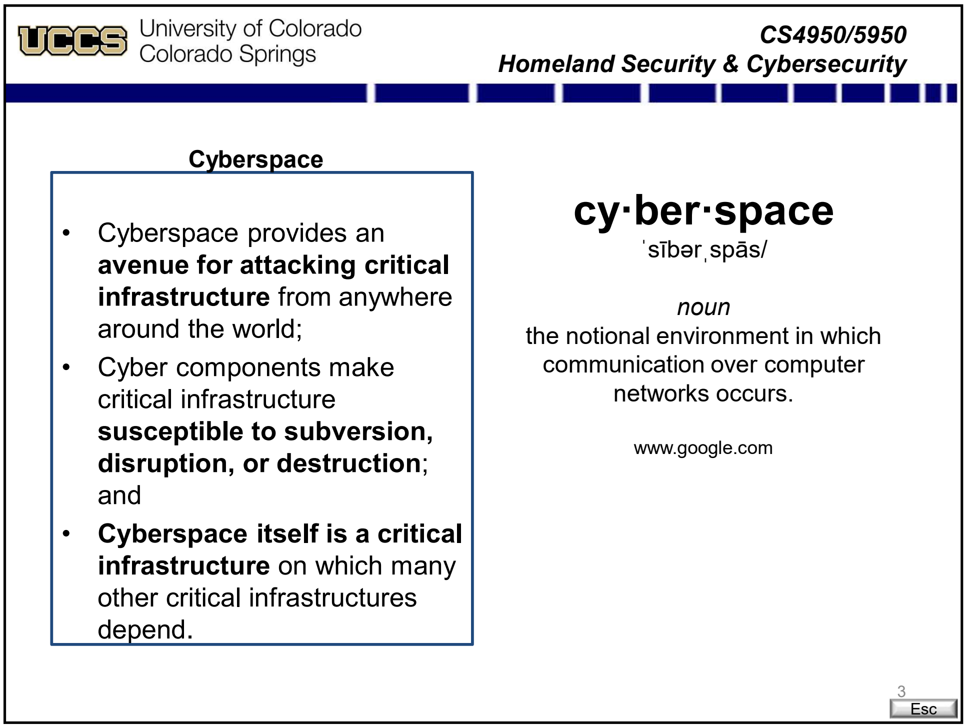
adjective
of, relating to, or characteristic of the culture of computers, information technology, and virtual reality.

synonyms: electronic, digital, wired, virtual, web, Internet, Net, online

www.google.com

2
Esc

2



University of Colorado
Colorado Springs

_CS4950/5950_
Homeland Security & Cybersecurity

Cyberspace

- Cyberspace provides an **avenue for attacking critical infrastructure** from anywhere around the world;
- Cyber components make critical infrastructure **susceptible to subversion, disruption, or destruction**; and
- **Cyberspace itself is a critical infrastructure** on which many other critical infrastructures depend.

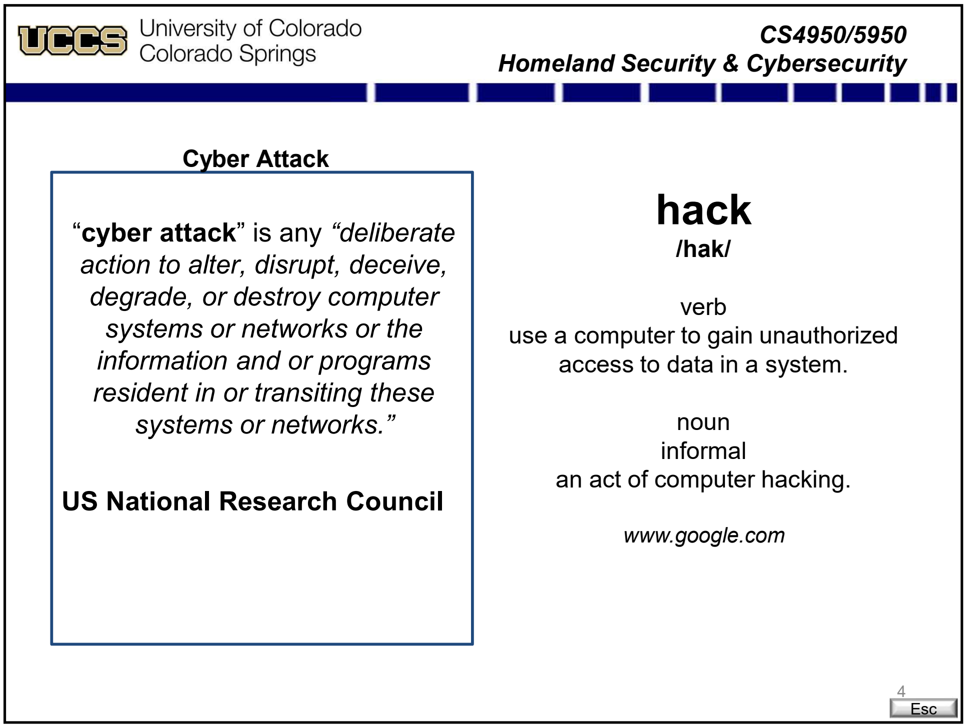
cy·ber·space
ˈsībərˌspās/

noun
the notional environment in which communication over computer networks occurs.

www.google.com

3
Esc

3



University of Colorado
Colorado Springs

_CS4950/5950_
Homeland Security & Cybersecurity

Cyber Attack

"**cyber attack**" is any *"deliberate action to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and or programs resident in or transiting these systems or networks."*

US National Research Council

hack
/hak/

verb
use a computer to gain unauthorized access to data in a system.

noun
informal
an act of computer hacking.

www.google.com

4
Esc

4

Cybersecurity

Title 18 Section 1030 United States Code, **prohibits unauthorized access** to computers used by the Federal government, banks, and otherwise used for interstate or international commerce.

1984 Counterfeit Access Device & Computer Fraud & Abuse Act

cybersecurity

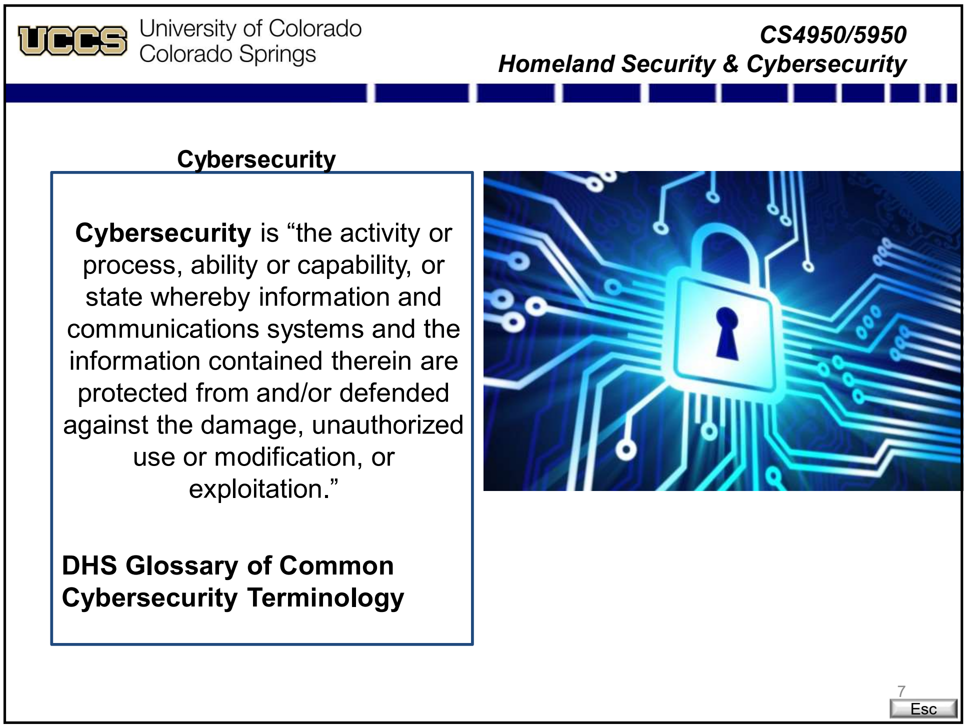
/ˌsībərsiˈkyo͝orədē/

noun
the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

www.google.com

Cybersecurity

- Due to the inter-state nature of the Internet, **the law is interpreted to mean most all computers and cell phones.**
- A 1986 amendment made it a further **crime to distribute malicious code, traffic passwords, or conduct denial of service attacks.**



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity

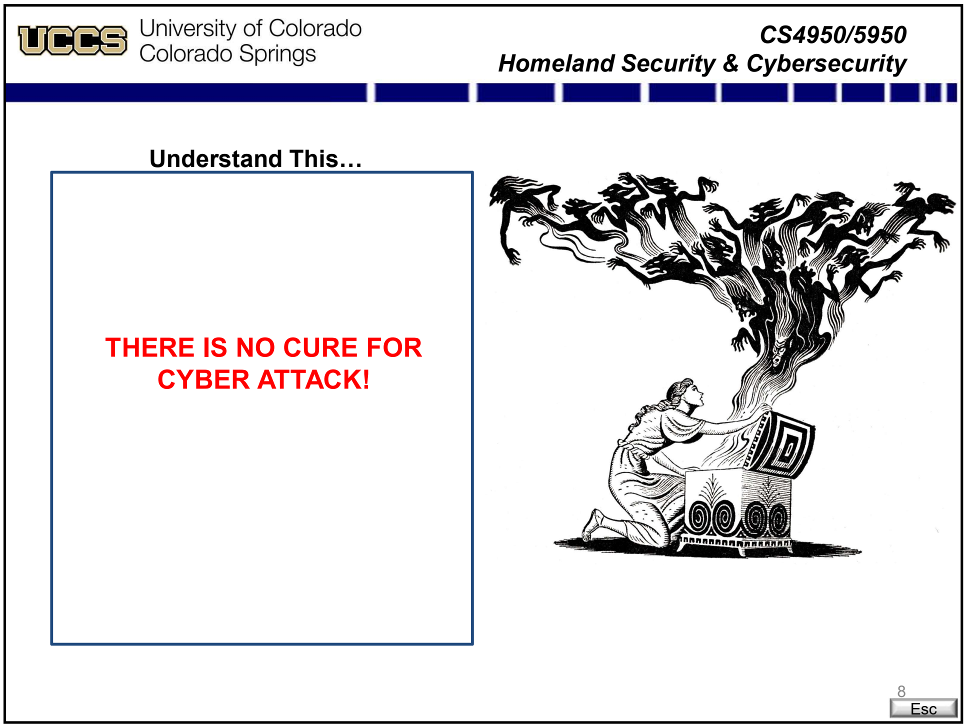
Cybersecurity is "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against the damage, unauthorized use or modification, or exploitation."

DHS Glossary of Common Cybersecurity Terminology

7

Esc

7



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Understand This…

THERE IS NO CURE FOR CYBER ATTACK!

8

Esc

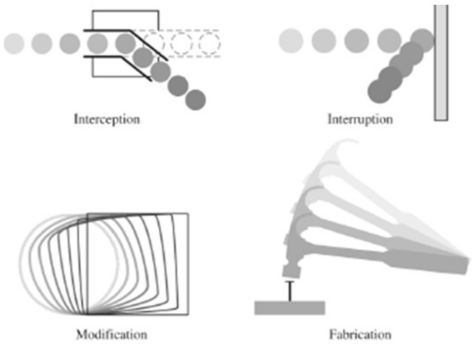
8

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity

- In concept, cybersecurity is about ensuring the confidentiality, integrity, and availability of a computer and its data.
- **Confidentiality** ensures that the system and data are not accessed by an unauthorized agent.
- **Integrity** ensures that the system and data are not corrupted by an unauthorized agent.
- **Availability** ensures that the system and data are always accessible when needed.



9
Esc

9

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity

These seemingly simple goals, however, are very difficult to attain because computers are inherently stupid and fragile.

10
Esc

10

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity

- **Computers are stupid** because unlike humans, computers are incapable of making value judgments regarding their actions and will perform as directed regardless of the outcome, even if the consequences are catastrophic.
- **Computers are also fragile**; a single wrong character can disrupt millions of lines of code.
- **Finding such flaws is impossible.**

11
Esc

11

UCCS University of Colorado Colorado Springs

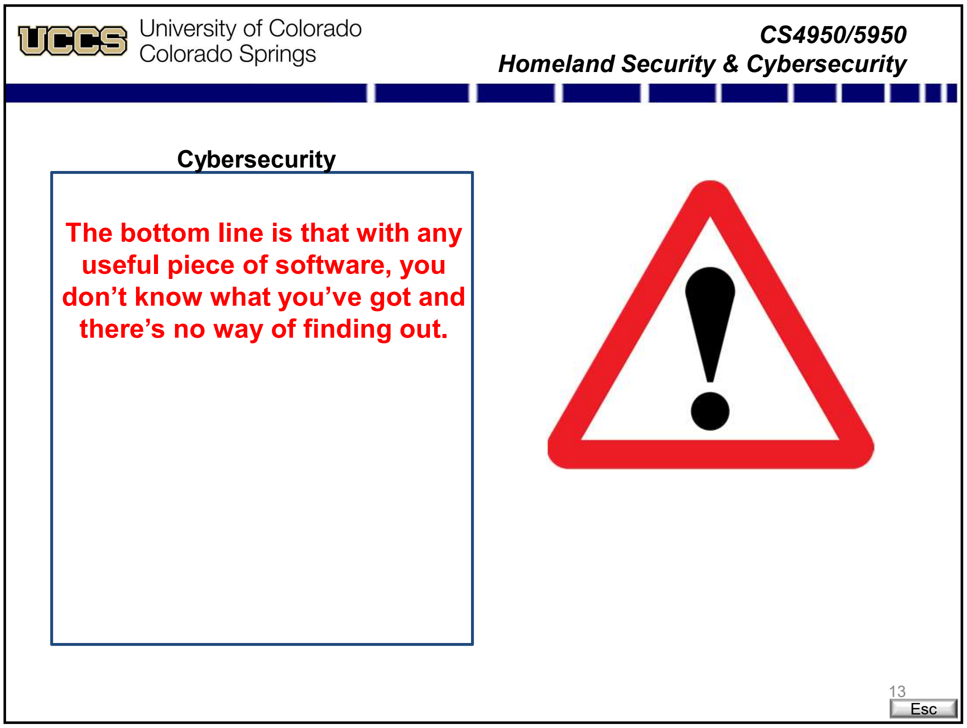
CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity

- **Even a small 100-line program** with some nested paths and a single loop may contain **100 trillion paths.**
- Assuming each path could be evaluated in a millisecond, that's 1,000 paths tested every second, **it would take 3,170 years to test all possible paths through the code.**
- **The Android operating system for mobile devices has 12 million lines of code.**

12
Esc

12



University of Colorado Colorado Springs

CS4950/5950 Homeland Security & Cybersecurity

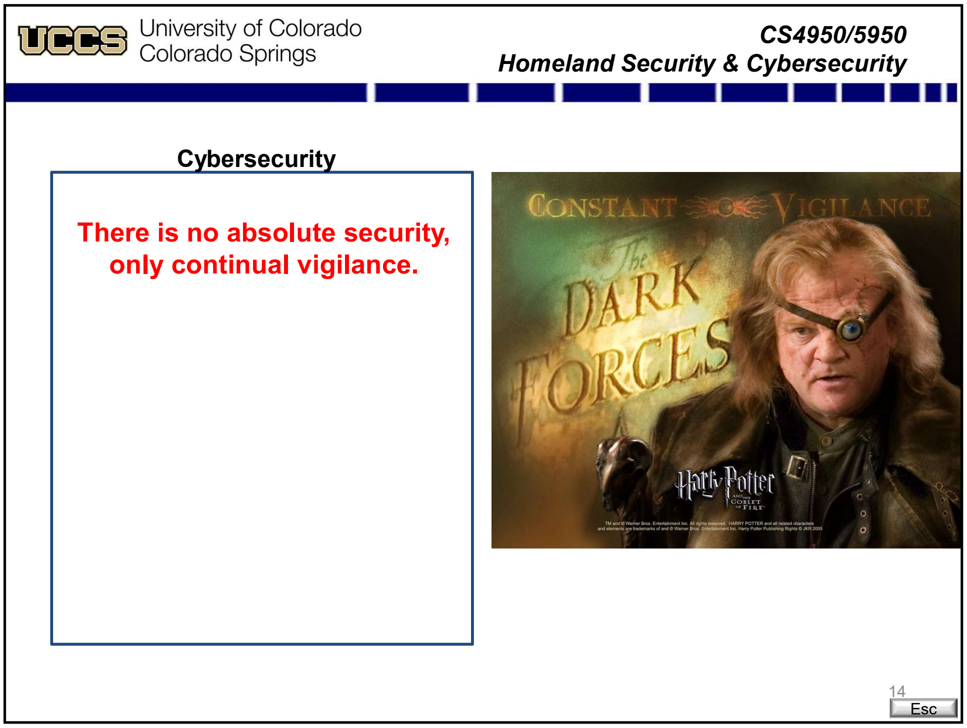
Cybersecurity

The bottom line is that with any useful piece of software, you don't know what you've got and there's no way of finding out.

13

Esc

13



University of Colorado Colorado Springs

CS4950/5950 Homeland Security & Cybersecurity

Cybersecurity

There is no absolute security, only continual vigilance.

14

Esc

14

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

DHS Cybersecurity

- **2002 Homeland Security Act** makes DHS responsible for national cybersecurity.
- However, **DHS has no control over computers** outside the Federal Government.
- You may ask DHS for help, but **their resources are very limited.**
- Moreover, **DHS has no more ability to make anything more secure than anybody else.**

15
Esc

15

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity Front Line

That is why today the first and last line of cyber defense rests with system owners and operators.

16
Esc

16

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Primary Hacking Methods

- **Exploitation**. Takes advantage of software flaws.
- **Phishing**. Try to steal somebody's credentials.

17
Esc

17

UCCS University of Colorado Colorado Springs

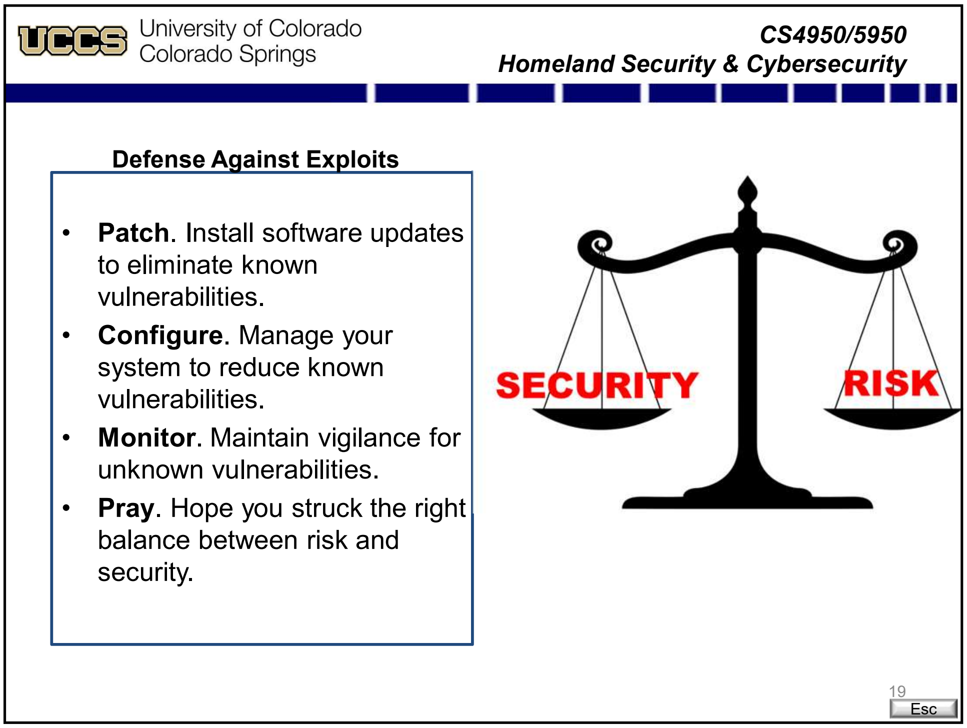
CS4950/5950
Homeland Security & Cybersecurity

Team Effort

- The best defense involves all members of the agency.
- IT protects your systems from exploits.
- Everybody protects your agency from phishing.
- Your defense is only as strong as your weakest member!

18
Esc

18

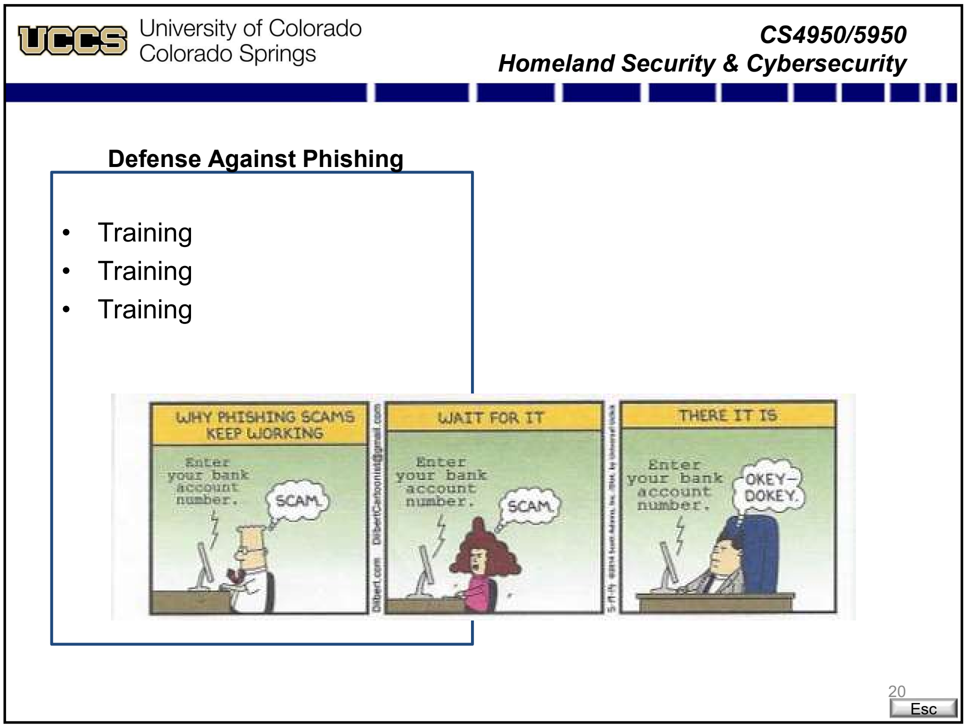


University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Defense Against Exploits

- **Patch**. Install software updates to eliminate known vulnerabilities.
- **Configure**. Manage your system to reduce known vulnerabilities.
- **Monitor**. Maintain vigilance for unknown vulnerabilities.
- **Pray**. Hope you struck the right balance between risk and security.



University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Defense Against Phishing

- Training
- Training
- Training

WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM
WAIT FOR IT
Enter your bank account number.
SCAM
THERE IT IS
Enter your bank account number.
OKEY-DOKEY.
Dilbert.com DilbertCartoonist@gmail.com

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Plan to Fail

- Backup & Recovery
- Insurance

There are only two types of systems: Those that have been hacked and those that don't know they've been hacked.

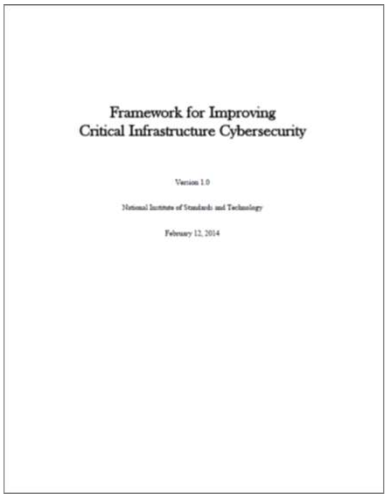
IF OUR BUSINESS PLAN FAILS, DO WE HAVE A PLAN FOR THAT?
ONLY LOSERS PLAN FOR FAILURE.
I THINK WE'RE ON THE SAME PAGE, BUT FOR SOME REASON YOU'RE ANGRY ABOUT IT.
Dilbert.com DilbertCartoonist@gmail.com
11-27-14 ©2014 Scott Adams, Inc. /Dist. by Universal Uclick

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Hope is Not a Strategy

- Approach cybersecurity in systematic manner.
- **Facilitates strategic planning.**
  - Where are you now?
  - Where do you want to go?
  - How are you getting there?
  - What is it going to cost?
  - What is the residual risk?

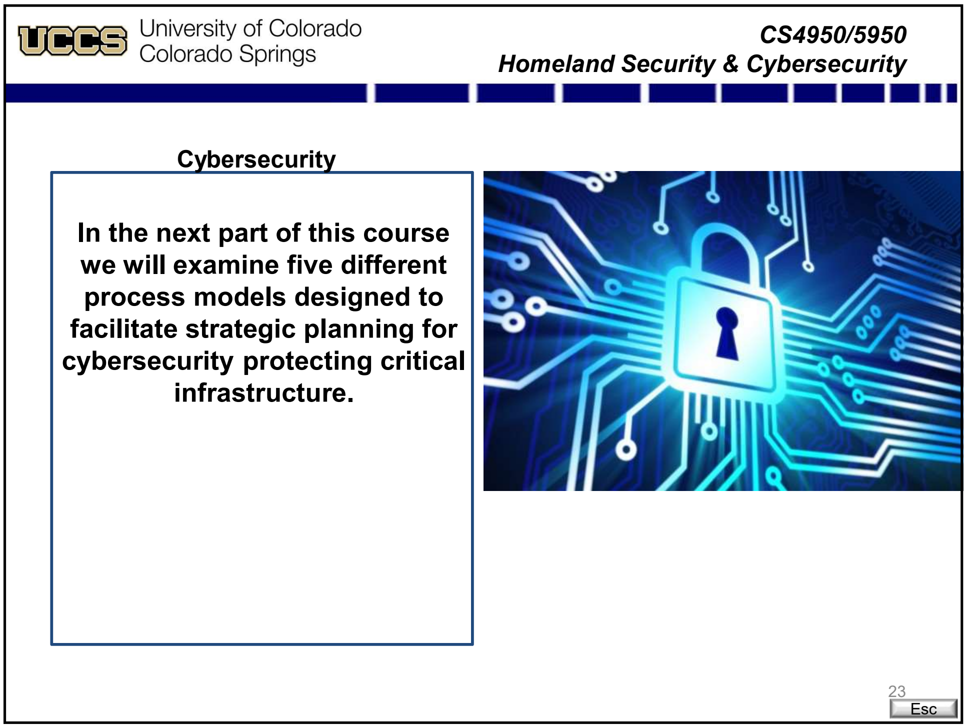


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

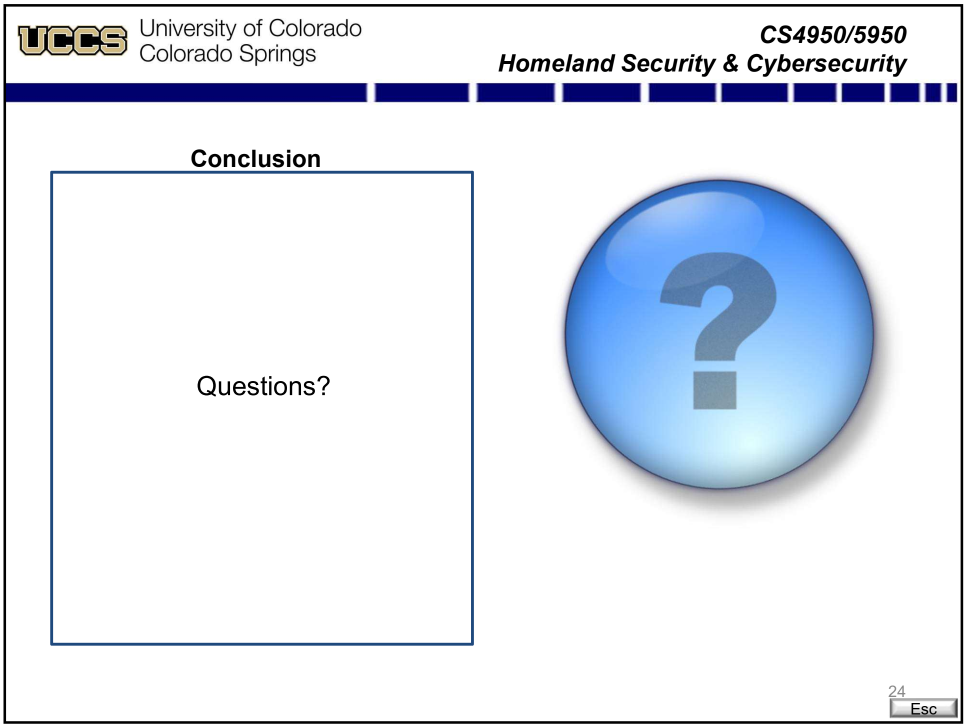
Cybersecurity

In the next part of this course we will examine five different process models designed to facilitate strategic planning for cybersecurity protecting critical infrastructure.

23

Esc

23



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?

24

Esc

24