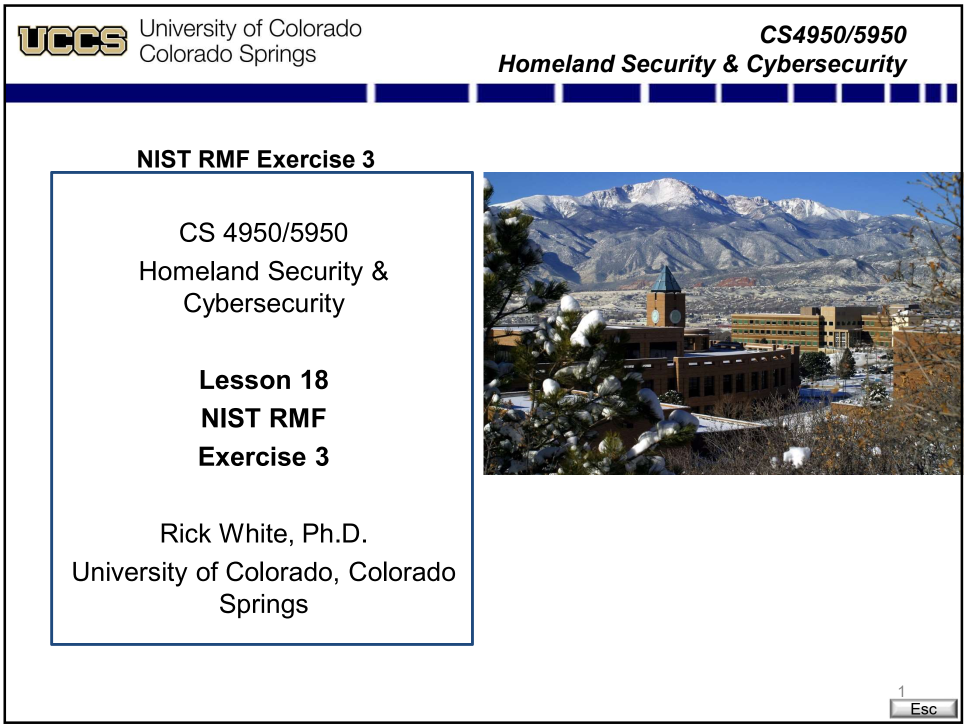


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

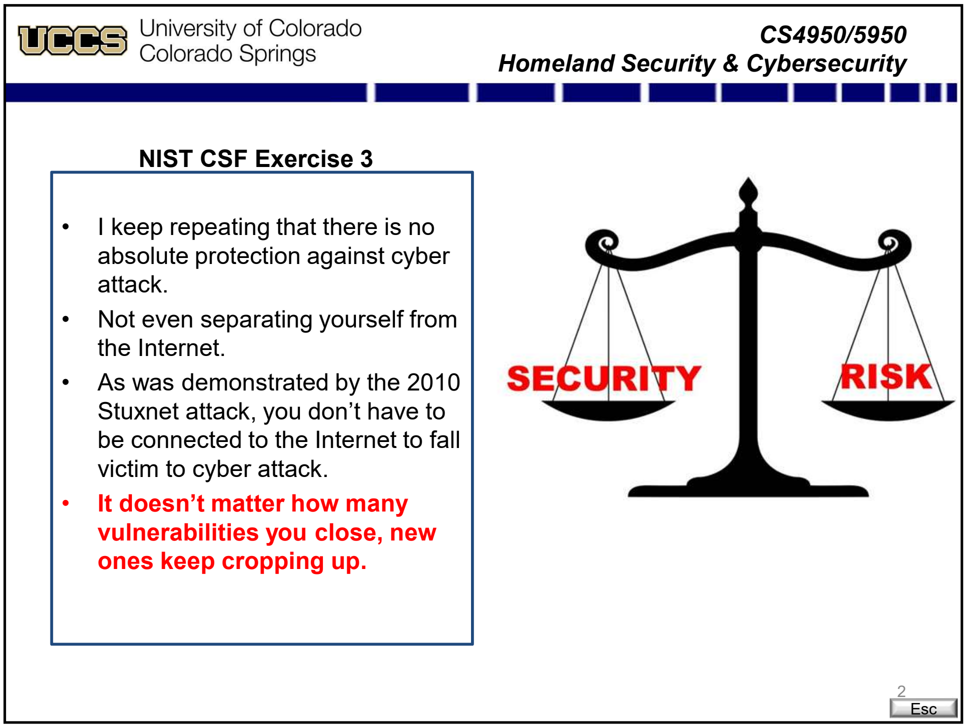
NIST RMF Exercise 3

CS 4950/5950
Homeland Security & Cybersecurity

Lesson 18
NIST RMF
Exercise 3

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

1



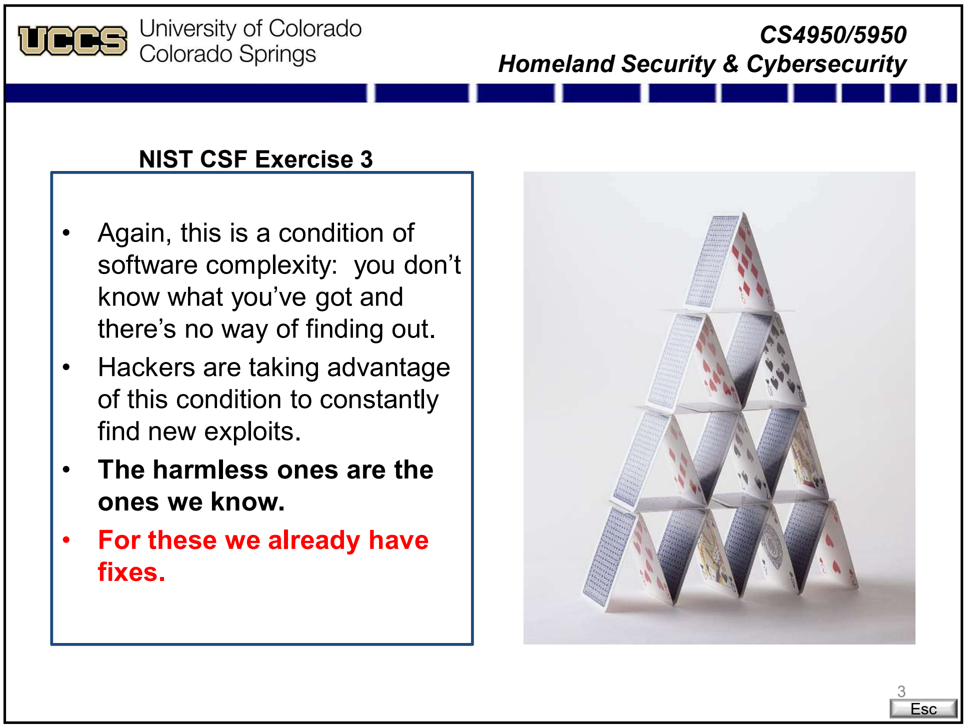
University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 3

- I keep repeating that there is no absolute protection against cyber attack.
- Not even separating yourself from the Internet.
- As was demonstrated by the 2010 Stuxnet attack, you don't have to be connected to the Internet to fall victim to cyber attack.
- **It doesn't matter how many vulnerabilities you close, new ones keep cropping up.**

2



University of Colorado
Colorado Springs

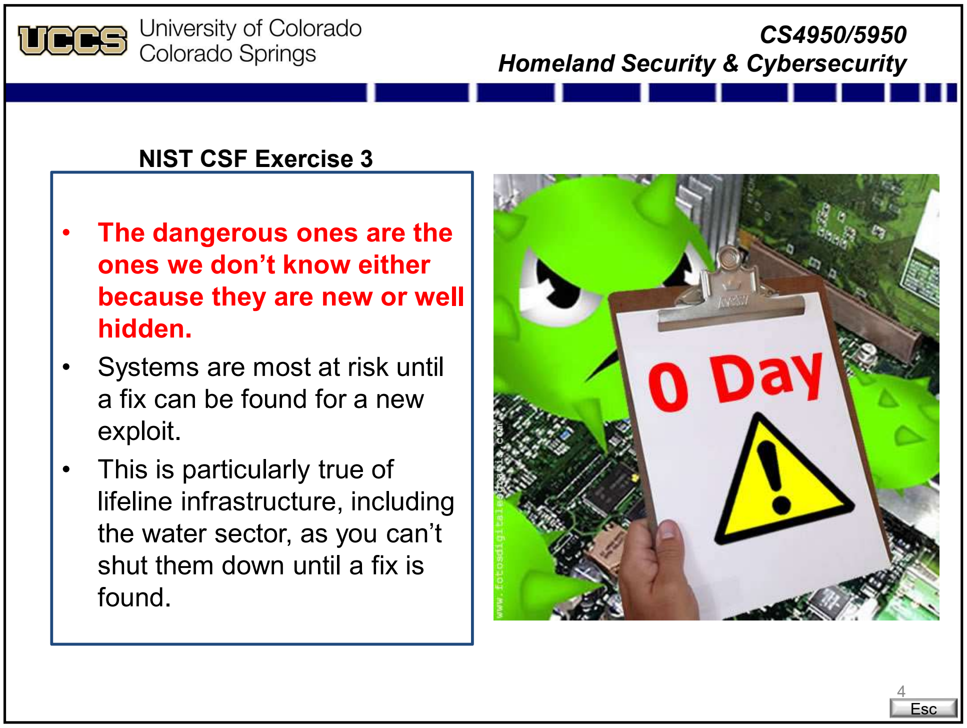
CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 3

- Again, this is a condition of software complexity: you don't know what you've got and there's no way of finding out.
- Hackers are taking advantage of this condition to constantly find new exploits.
- **The harmless ones are the ones we know.**
- **For these we already have fixes.**

3
Esc

3



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 3

- **The dangerous ones are the ones we don't know either because they are new or well hidden.**
- Systems are most at risk until a fix can be found for a new exploit.
- This is particularly true of lifeline infrastructure, including the water sector, as you can't shut them down until a fix is found.

4
Esc

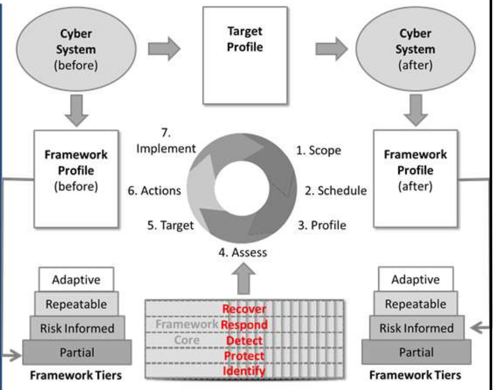
4

NIST CSF Exercise 3

Accordingly, the NIST Cybersecurity Framework recognizes that **it is only a matter of "when", not "if" a cyber attack will succeed.**

NIST CSF Exercise 3

This recognition is built into the Framework Core which is functionally organized into cybersecurity measures designed to **identify, protect, detect, respond, and recover.**

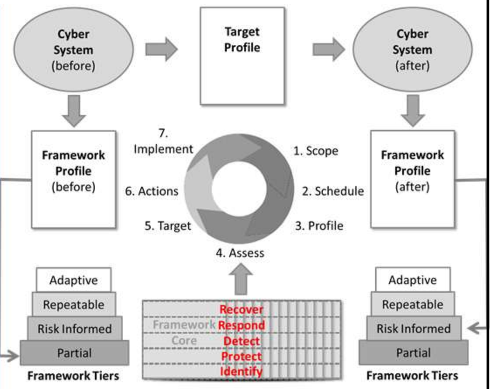


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 3

Question: Of these five functions, which one do you think is most important?



7
Esc

7

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 3

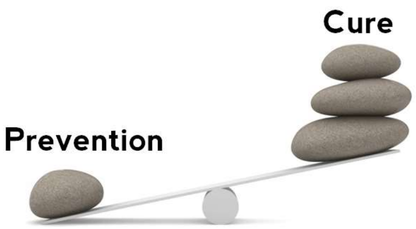
In this case I will concede that an **acceptable answer is "it depends",** but allow me to make the case for one function in particular.

8
Esc

8

NIST CSF Exercise 3

- While the old adage is true, “an ounce of prevention is worth a pound of cure”, consider that all the prevention in the world will not prevent a successful cyber attack.
- **By this argument, measures taken to identify, protect, detect, and respond to cyber attack can only ever be partially effective.**
- **On the other hand, the means for recovery are completely within your control.**



Copyright © Pegasus Vertex, Inc

NIST CSF Exercise 3

The most difficult part is making the business case to management.

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 3

- For good reasons, most management is conservative, making them more likely to lean towards prevention than recovery.
- I am certain more than one System Security Officer has been told that **"failure is not an option".**
- Unfortunately, **failure is all too likely an option.**
- **This point has to be made to management.**

YOU'VE GOT A BAD CASE OF MANAGER'S ELBOW.
IT'S CAUSED BY PATTING YOURSELF ON THE BACK AND COVERING YOUR BUTT AT THE SAME TIME.
I RECOMMEND THAT YOU JOIN THE CIRQUE DU SOLEIL. I'M GIVING YOU A PRESCRIPTION FOR A LEOTARD.
www.dilbert.com
scottadams@aol.com
7-9-05
©2005 Scott Adams, Inc./Dist. by UFS, Inc.

© Scott Adams, Inc./Dist. by UFS, Inc.

ALL YOU DID THIS QUARTER IS DESIGN ONE MICROCHIP.
IN COMPARISON, I FOUND THE TIME TO ATTEND DOZENS OF MEETINGS.
NOW DO YOU SEE WHAT IT TAKES TO BE A MANAGER?
SADLY, YES.
www.dilbert.com
scottadams@aol.com
4-19-05
©2005 Scott Adams, Inc./Dist. by UFS, Inc.

© Scott Adams, Inc./Dist. by UFS, Inc.

11

Esc

11

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 3

- Once they understand this fundamental point, then the business case can be made in terms of losses as a function of down time.
- **The shorter the down time, the smaller the losses.**
- If you can make your recovery fast enough, **theoretically you can drive your losses down to zero.**
- That's not going to happen.

12

Esc

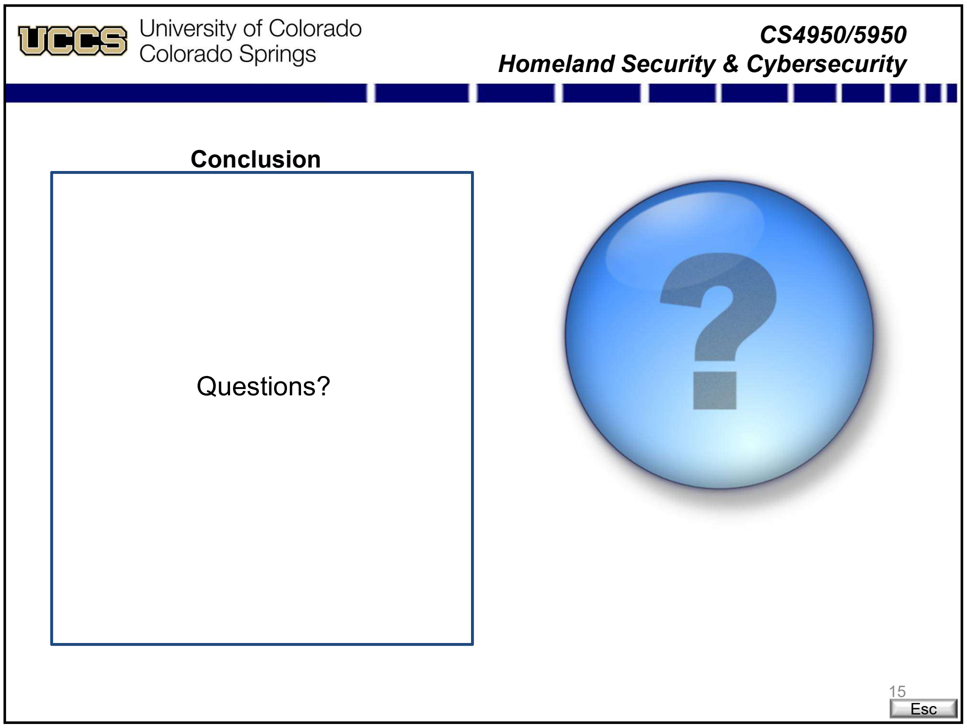
12

NIST CSF Exercise 3

- There will always be some loss.
- But the point of this lesson is that as a hard-charging System Security Officer **you're going to be under management pressure to avoid failure at all costs.**

NIST CSF Exercise 3

- **The better strategy is to accept the inevitability of failure, and invest in measures that expedite recovery.**
- **This will require some convincing on your part.**



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?

15

Esc

15