

UCCS University of Colorado
Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity

NIST RMF Exercise 2

CS 4950/5950
Homeland Security &
Cybersecurity

Lesson 18
NIST RMF
Exercise 2

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



1
Esc


1

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 2

You are the System Security
Officer for a municipal water
department that supplies drinking
water for about 9 million residents
in a large east coast city.



2
Esc

2

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 2

Your department operates two independent treatment plants that together supply over a billion gallons of clean water daily.

Control System

3 Esc

3

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 2

- Both facilities receive their water from separate sources and have their own distribution systems, but are **cross-connected to provide complete backup support when one facility requires maintenance or is otherwise shutdown.**
- After 9/11, your department started receiving Department of Homeland Security grant funding under the **Urban Area Security Initiative.**

Control System

4 Esc

4

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 2

- In 2014, department management allocated UASI funds to start implementing the NIST Cybersecurity Framework.
- Over the past several years, your office has succeeded in completing two cycles of the Framework Process, and now assess your Current Profile at Tier 3, "Repeatable".

5 Esc

5

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 2

- This means that your cybersecurity practices are part of the department's formal business process;
- Your cybersecurity program is continuous and responsive to change; and
- Suppliers are included in your cybersecurity program.
- So here you are, three years into a successful program conducting your annual business review when management asks **what's your goal for the next year?**

6 Esc

6

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 2

Should you try to attain a Tier 4 “Adaptive” Target Profile?

7 Esc

7

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 2

- Because of your familiarity with the Framework Core, you already have a pretty good idea what additional measures would be required.
- **You also know that these measures would necessitate the hiring of additional personnel, which would put you at least 20% over budget.**
- **By your estimate, the security gains would be marginal.**

8 Esc

8

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 2

- **Of course department management always wants “the most” security, even if the gains are marginal.**
- Their worst nightmare is something going wrong that in hindsight could’ve been prevented.
- **Maybe they would approve a 20% budget increase for your office.**

9 Esc

9

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 2

- **What do you recommend?**
- Should you push for the next tier level or remain where you are?

10 Esc

10

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 2

- If you said “push for the next level, and go for Tier 4”, you were probably motivated by the potential consequences of a successful cyber attack shutting down the water supply.
- They would indeed be catastrophic.
- But in this case I would have to disagree.**

11 Esc

11

UCCS University of Colorado
Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 2

- Remember, all cybersecurity is about risk management.**
- The first rule of cybersecurity risk management is that **there is no absolute security.**
- Given the current state of technology, **there is always a risk of successful cyber attack** no matter what security measures you put in place.
- There is no guaranteed protection against a “zero-day” virus or “insider” attack.**

12 Esc

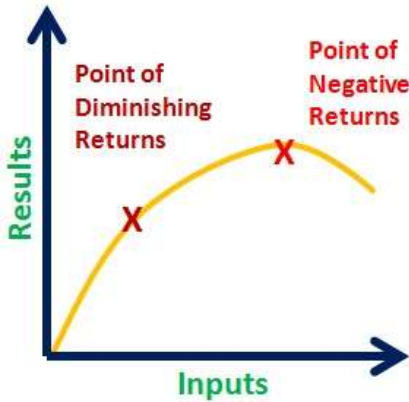
12


 University of Colorado
 Colorado Springs

CS4950/5950
 Homeland Security & Cybersecurity

NIST CSF Exercise 2


- The question then becomes one of cost-benefit-analysis.
- **Eventually, you start gaining less protection at higher cost; you run into the law of diminishing returns.**
- Cost-benefit-analysis determines at what point the perceived benefits don't justify the associated costs.



13

Esc

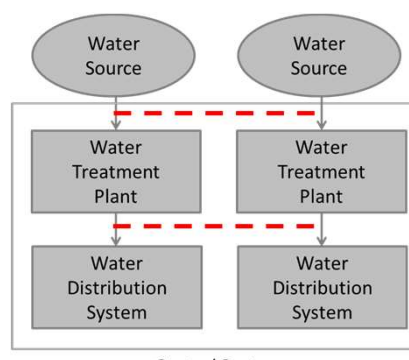
13


 University of Colorado
 Colorado Springs

CS4950/5950
 Homeland Security & Cybersecurity

NIST CSF Exercise 2


- But this is not necessarily the System Security Officers' decision to make.
- **Management will make the decision**, they are just looking to you for the best advice.
- **My recommendation would be to stay put at Tier 3**, and I would explain the reason for my recommendation.
- **If management still chooses to push on to Tier 4**, then that's their decision based on the best information currently available.



14

Esc

14




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


NIST CSF Exercise 2

Again, they are operating in the light and not in the dark.



15
Esc

15




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?



16
Esc

16