Week 1

1. Professor Andrew Calhoun is an expert at \*cyber\* \*defense\*.

2. The first thing Dr. McIver learned in his most recent Security job is that there is no \*shame\* in being a \*cybersecurity\* professional.

3. The missing artifacts that organizations/firms should have is there \*Logs\*, \*network baselines\*, \*infrastructure drawings\*, \*network maps/network map\*, and \*change control configurations\*.

4. \*No\*, \*security-minded/security minded\* administrators are enough to \*secure\* a network?

5. Professor Calhoun says that you have to devote \*time/energy/money\*, \*energy/time/money\*, and \*money/time/energy\* to cybersecurity.

6. A letter to the \*CFO\* is the assignment that Professor Calhoun gives his students to perfect their professional \*communication\*.

7. According to Dr. McIver, this is a good assignment because \*degree\* holders are in \*leadership\* roles and \*executive\* communications are incredibly important.

8. According to Professor Calhoun, a Cyber Defender is an \*operator\* whose sole goal is to \*protect\* assets they are trying to safeguard on a network.

9. According to Dr. McIver, cybersecurity is like having a good \*security\* system, response system, \*barriers\*, and passive personnel. \*Defense\* is the \*active\* protection of a person, place, or a thing.

10. A 3-4 person \*team\* is a good size for a \*Cyber\* Defense team.

11. \*Host\* Analysts and \*Network\* Analysts are the 2 cyber defense roles that Professor Calhoun mentions. One is \*micro\* focused on the hosts and the other is \*macro\* focused on the big \*picture\* of the overall \*network\*.

12. \*Security Onion\* is the cyber defense tool that was recommended to Dr. McIver.</p>

13. According to Dr. McIver, \*Security\* Onion is like Kali \*Linux\* on the Blue side.

14. \*Firewalls/ACLs/Access Control Lists/IDS/IPS\*, \*Firewalls/ACLs/Access Control Lists/IDS/IPS\*, \*Firewalls/ACLs/Access Control Lists/IDS/IPS\* are some Cyber Defense tools that Professor Calhoun mentions.

15. A cyber defender's goal is to \*Prevent/Protect/Limit Risk\*, \*Prevent/Protect/Limit Risk\*, \*Prevent/Protect/Limit Risk\*, and limit Data Loss.

16. Defensive \*tools\* are used for limiting the chances that an \*attacker\* has at getting what they want.

17. \*Attackers\* want \*Unauthorized Access/Information/Maintaining Persistence\*, \*Unauthorized Access/Information/Maintaining Persistence\*, and \*Unauthorized Access/Information/Maintaining Persistence\* on your network.

18. Dr. McIver mentions that Cyber Defender's additional roles are to \*inspect/detect\*, \*inspect/detect\*, and remove.

19. Some of the tools that remove attackers are \*cutting/blocking\* ties to an IP address, \*removing/deleting\* files that aren't supposed to be on your network.

20. A defender would not remove an attacker if they wanted to \*monitor/see/watch\* the \*attacker's/attacker/attackers\* activity.

21. According to Dr. McIver, the two biggest things in cybersecurity that can be used to defend against \*APT/APTs\* are \*OPSEC/Operational Security\* and Cyber \*Hygiene\*.

22. Cyber Hygiene is \*Patching/Scanning/User behavior/Admin behavior/Adminstrator behavior\*, \*Patching/Scanning/User behavior/Admin behavior/Adminstrator behavior\*, \*Patching/Scanning/User behavior/Admin behavior/Adminstrator behavior\*, and \*Patching/Scanning/User behavior/Admin behavior/Adminstrator behavior\*.

Week 2

1. According to Dr. McIver, the only way to build a \*CIO\*, is to create a Service Desk \*Supervisor\*, IT Manager, and an IT \*Director\*.

2. According to Dr. McIver, \*Risk\* Management is called the Universal Language of \*Business\*.

3. Prof Scott mentions that the \*business side\* is inherently dangerous because they are handling people's lives, data, and \*information\*.

4. Prof Scott highlights the focus of the business side by saying, The business side says where is the \*stakeholders\*, \*stockholders\*, \*customers\*, and employees.

5. Prof Scott says that in business the IT guy is the CIO and is focused on \*decision\* making \*data\* management, and data \*security\*.

6. Speaking on business opportunity, Prof Scott mentions two things: The cost of \*failure\* and the cost of \*not even trying\*.

7. Prof Scott says that \*Cybersecurity Risk\* is Business Risk and it should be in the decision making of all business professionals.

8. Dr. McIver says that we live in an era where \*CISOs\* can no longer say NO. Prof Scott says the appropriate response is Yes... \*But\*

9. According to Prof Scott, The CISO \*facilitates\* the \*acceptance\* of Risk and/or mitigation of risk by saying what do you risk by doing this?

10. Prof Scott says that CISOs report to the \*success\* of the business.

11. Dr. McIver stresses that, saying No allows the competitor to get \*ahead\* of you, let's the \*customer\* down, and no leads you to \*hiding\* in your shadow.

12. Dr. McIver's mantra is, we are going to do this, yes, but we are going to do this the \*right way\*.

13. Dr. McIver thinks that... If you want to just pound a keyboard you can join a company that \*solely\* does IT. If you do IT for a company, you are not a \*traditional\* IT professional, you are a Network \*manager\*, planner, \*cloud\* broker, service \*provider\*, or ITIL \*professional\*.

14. Prof Scott believes that CEOs must told that the \*security\* of the network is not an IT decision because it enables decision-making, \*analysis\*, customer \*trust\*, customer actions, all of the things that drive \*success\*.

15. According to Prof Scott, we have to teach \*technicians\* to speak to the business \*relevance\* to the decision otherwise they are just techies.

16. During the CapEX/OpEX discussion, Prof Scott says that when we outsource our infrastructure to the cloud it is not a \*Capital\* Expense because you did not have put out the original outlay but it's an \*Operational\* Expense because you pay a monthly fee.

17. Dr. McIver says that the fallacy is that if we go from CapEx to OPex is that we are going to \*save\* money.

18. Prof Scott says that The biggest threat to Cybersecurity is our own \*users\*. Dr. McIver thinks that it is the \*administrators\*.

19. Prof Scott says, You have to build the \*culture\* that your Cybersecurity is the business it enables the business.

20. Dr. McIver says that he read that the \*home\* is the new attack surface. This is a risk because users are blending their home \*devices\* and their \*work\* devices.

21. According to CIO.com, CIOs are requiring \*degrees\* less and less. Dr McIver thinks that is a mistake because he needs professional \*learners\* and diversity of thought.

22. Prof Scott thinks CIOs are abandoning degree requirements because there are a lot of great learning tools out there. If is a person can prove that \*they know\* their stuff the CIO is satisfied but, in the \*boardroom\*, they may not get that opportunity.

23. Dr. McIver personally believes that, IT \*Leaders\* do all of the things that IT technicians and Engineers don't want to do. Their job is to bring \*IT\* to Business and \*Business\* to IT.

24. Prof Scott says that IT leaders are enabling success, but it is the business success. The IT professional must show up every day and \*prove\* their value to business \*success\* not just to keep the technology working.

Week 4

1. According to Prof Nop the \*Security\* Footprint of Databases is \*large\*.

2. This is because of \*misconfiguration\* like installing a bunch of things that you don't need.

3. That increases your security footprint becuase it is more \*maintenance\* and you can forget to \*update\* everything because you are focused mostly on what you use often.

4. Prof Nop says that people create databases with \*excess\* administrative privileges.

5. According to Prof Nop, Just like any code, when you don't have something to \*sanitize\* the data coming in, the result is having \*code\* that is susceptible to \*injects\* that can damage your application.

6. According to Dr. McIver, “Just win baby”; works in \*football\* but doesn't work in \*cybersecurity\*.

7. When you ignore the \*confidentiality\* and \*integrity\* portions of the CIA triad it ultimately impacts \*availability\*.

8. Prof Nop says that a threat actor may not want to take down your system but \*manipulate\* the data in your system leading to bad decision making.

9. We (cybersecurity professionals) always want all 3 parts of the CIA triad but the \*business\* side needs to pick 1 to prioritize.

10. It is Prof Nop’s advice that when you think about availability, think about that \*critical\* system that can't go down.

11. \*Banking\* is the industry that Dr. McIver hesitant to do cybersecurity for

12. Prof Nop treats a \*Database\* is like a production system, you don't want to mess with it while its being worked in.

13. Prof Nop says running the database in \*development/test\* or \*test/development\* version is a way to ensure that security won't break a database.

14. Prof Nop says the DevSecOps is possible because you can run code through a \*pipeline\* and run security checks to ensure that the syntax is correct, check for \*vulnerabilities\*, and check for unsecure configurations.

15. Cybersecurity pros need to be honest about “can't” vs “won’t'” when it comes to updating \*older/sensitive\* or \*sensitive/older\* systems.

16. Prof Nop says that you can build \*security\* around a sensitive database that can't be \*modified\* for security purposes.

17. Prof Nop says that there is no such thing as a \*free\* lunch. In order to get something, you have to \*give\* something.

18. Dr. McIver says that the \*CISO\* is responsible for protecting the database, but business makes the \*decision\* to protect it.

19. Prof Nop uses \*segregation\* to protect the database from other parts of a network and says that if you have sensitive information don't put it in the \*DMZ\*.

20. Prof Nop says that you can also create separation by having different \*instances\*, data in different \*tables\*, or implementing different \*permissions\*.

21. Dr. McIver didn't understand how important \*databases\* were because he was focused on operations and hardware. Prof Nop says that working on databases are hard because the code is so \*sensitive\*.

22. Prof Nop's final bit of advice is, utilize \*Operating\* System security actions on the \*Database\* Management System. In the IT world, they segregate the \*network\*, that can also be adopted in the management of databases. \*Encrypt\* your sensitive data. Database Management Systems now have features that allow for \*Role\* Based Access \*Controls\*, creation of \*policies\* in the database environment, \*auditing\*, or logging. Logging allows you to determine what happened to your database.,

Week 6

1. Prof Nop works for a company that is responsible for consumer \*healthcare\*.

2. His title is \*security\* operations center manager and is responsible for \*detection\* and \*response\*.

3. Intelligence is \*analyzed\* information that \*helps\* you do your job and make \*decisions\*.

4. Dr. McIver uses the term \*actionable\* intelligence instead of \*cyber\* intelligence.

5. Dr. McIver performs \*Business\* and \*Geospatial\* Intelligence in his intelligence practice as a Chief Data Officer.

6. Actionable intelligence tells you when it \*might\* happen and if \*something\* happened that you should be concerned about.

7. It allows you to look at your \*organization\* and how to button up your network.

8. Cyber Intelligence helps you focus your \*resources\*, what kinds of \*controls\* to put in place, and \*inform\* you of vulnerabilities that help you use your tools that you already have.

9. You need to have strong \*analytical\* skills to be a cyber \*threat\* analyst. It is not something that is easy to get in and out of and call yourself an \*expert\*.

10. According to Dr. McIver, the analytical \*skillset\* that you gain is unmatched like how to analyze, \*sift\* through, and never give up on \*information\* that could be critical to \*inform\* decision-making.

11. Dr. McIver says that intelligence is \*analyzed\* and \*applied\* information.

12. Prof Nop says that a Master's student who projects to be a leader without extensive technical skills, you need to understand the big picture, everybody is a \*producer\* of intelligence and a \*consumer\* of intelligence.

13. The upper echelon has to know that you have to \*plan\*, \*direct\*, and \*steer\* intelligence and \*align\* it to your business.

14. Dr. McIver says that at some point we all have to transition from \*tech\* to business. In order to survive, we have to learn how to take tech to business and \*business\* to tech.

15. Dr. McIver says that the \*craftiness\* and understanding the business \*value\* will drive the \*intelligence\* that you require.

16. Dr. McIver's boss used to say in response to a threat “what's the \*likelihood\*?”

17. Dr. McIver's boss used to say in response to the likelihood, "what the \*impact\* if it happens?”

18. When Dr. McIver told the impact, his boss would "say what's the most \*likely\* impact"

19. This made Dr. McIver look at intel \*differently\* and say give me the \*highest\*, the lowest, and the medium impact, likelihood, and \*threat\*.

20. Prof Nop agrees that there is \*conflict\* in sharing intelligence when \*intellectual\* property is involved. Proj Nop said that you must get the \*lawyers\* involved because \*safety\* is number 1. This is something that can also be prepared for.

21. In Prof Nop's experience, intelligence should be viewed as an \*enabler\* and drives \*operations\* if you use it \*correctly\*. When you allow intelligence to drive operations you will be a lot more \*successful\*.