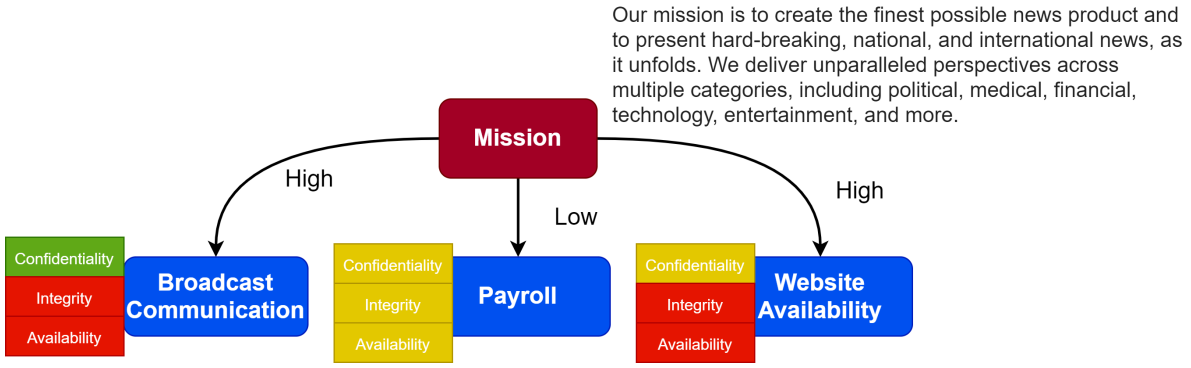
Vulnerability Defender

The purpose of this workout is to familiarize you with the security properties of *confidentiality*, *integrity*, and *availability*. When asked the question, “Is this secure?”, these properties help to better define what we mean by *secure*. But to make these properties meaningful, we need to tie them to something. For organizations, this means their mission or the reason they exist.

Let’s start with an example. In the figure below, we take a few sample systems from a news agency. We find their mission statement and keep it in front of us. Then we ask ourselves what a loss of *confidentiality, integrity*, and *availability* for the system would mean for the mission of the organization. In this example, green stands for no impact, yellow stands for low impact, and red stands for high impact. The final label for the mission defaults to the maximum impact of all 3.



Before moving on, let’s recap on the terms of *confidentiality, integrity*, and *availability.* Outside of cybersecurity, those don’t have a lot of meaning. It’s often helpful to take the system you are assessing and create a scenario tied to each of those terms. The table below is an example of scenario statements that help to determine mission risk. With scenarios, it’s easier for managers to make decisions about risk.

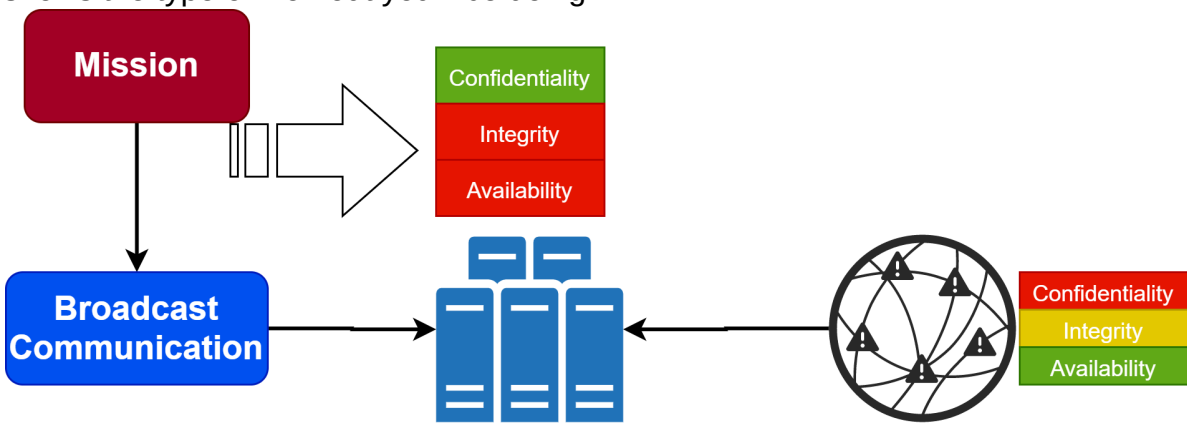
Term	What it means	The scenario for Broadcast Communication
Confidentiality	Secrecy of data	Malware on the network is exfiltrating data on the servers transmitting the broadcast
Integrity	Trust in data and systems	An adversary has remote control of the broadcast servers and has the ability to modify the transmission stream

Availability	Data and systems available when needed	The servers go down from a DDoS attack during a critical broadcast time period

So now, instead of “Is this secure?” we know a little more about what that means for each particular system. These are the building blocks of understanding cybersecurity risk.

This workout goes one step further. Instead of just categorizing the mission risk, you will be asked to make risk decisions about real vulnerabilities. These vulnerabilities come from the National Vulnerability Database and we refresh these nightly so you can work out many times without seeing the same one.

Vulnerabilities apply to individual system components, and they get reported with the same impact categorizations you use for mission risk. This makes it easier to determine an overall risk category for each vulnerability. The following image shows the type of workout you’ll be doing.



In the diagram, you can see how the mission risk we categorized above gets applied to individual systems. Vulnerabilities also apply to individual systems. In fact, it’s not uncommon for hundreds or even thousands of new vulnerabilities to apply to a system each month.

Now, each of these vulnerabilities has its own categorization for confidentiality, integrity, and availability. For example, a vulnerability on a web server disclosing a private web page would have a **high** confidentiality impact, and maybe a **low** integrity impact, but would probably have the category of **none** assigned to availability.

You can categorize the overall vulnerability by combining each of the security properties of the system with those of the vulnerability. A system with no confidentiality risk tied to the mission combined with a vulnerability of high confidentiality risk would have an effect of “**NONE”** on the mission. To come up

with the vulnerability risk, you would take the maximum of the combined vulnerability properties.

Level 1 provides the vulnerability characteristics for you so you can easily see how they combine with the mission. Then, in level 2, you are only given the vulnerability descriptions, from which you can then derive the security properties. For each answer you receive the following:

Risk	Points for Correct Answer	Points for Incorrect Answer
None	1	-1
Low	2	-2
High	3	-3

When you have finished level 2, you will automatically be taken to a completion screen showing the full results.