Effective Cyber Leadership: Avoiding The Tuna Fish Effect and Other Dangerous Assumptions

Andy Cohen

There is a joke in Hollywood that goes something like this:

God informed Mother Teresa that he would like to grant her anything she wished for all the wonderful work she had done.

"Would you like your own house?" he asked.

"I have lived my whole life without one. Got along fine. No thanks," she responded.

"How about money?" God offered.

"Never needed money," she answered.

"Isn't there anything you'd like that I can give you?" he asked in frustration.

"Well, there is one thing," replied Mother Teresa.

"Name it," God said excitedly.

Shyly, she responded, "I'd like to direct."

When I owned my advertising agency, I too got the opportunity to pursue a dream of directing. In this case, it was for an advertising commercial, and it taught me a leadership lesson I will never forget.

We had been shooting for hours when my producer pulled me over and said we needed to take a half-hour break. "The crew needs it, and it's Union rules," he informed me. My assumption was that a break wasn't necessary and that with the right inspiration, the crew could finish up shortly, saving us money. So, ignoring the advice of the producer, I pulled the entire crew together and gave them what I felt was a highly motivational speech about how great they were doing, how I believed they were up for the challenge, and how if we pulled our energies together, we could finish up shortly.

Andy Cohen is an entrepreneur, best-selling author, and international AI/Cybersecurity Behaviorist. His TEDx talks and workshops are world-renowned and include appearances at The Army Cyber Institute Conference, Google, HSBC China, and The World Bank. He has a degree in experimental psychology and a room full of esteemed advertising awards for finding creative solutions that drive measurable sales. Andy is the Chief Assumption Officer of Andy Cohen Worldwide, a global advisory firm helping organizations make faster, better decisions and enhance critical thinking. Between engagements, Andy teaches at the world's most respected universities. Colonel (Ret.) Greg Conti, Ph.D. called Andy's new book, *Challenge Your Assumptions, Change Your World,* "a must-read for the security professional." *Follow the Other Hand,* Andy's first book, was a *New York Times* notable read and has been translated into multiple languages.

Four hours later, we were still shooting. It was a disaster. By ignoring my producer's advice, I ended up with an angry and tired crew whom I paid time and a half, eating thousands of extra dollars out of our budget.

Leadership Is About Directing People

Leadership is all about motivating people to march in particular ways that achieve desired results. To do so effectively, however, we must admit that sometimes we assume the world thinks just like ourselves and shares the same motivations. As a result, we can lack the patience, empathy, and/or sensitivity to listen to what others who are closer to the problem have to say. Our assumptions driving "a win" often move us further from the solution instead of bringing us closer to the answers we seek.

The following cyber case illustrates this point. Due to the sensitive nature of this story, it will be told in general terms to protect those involved. Essentially, about thirty FBI and U.S. Postal Inspection Service (USPIS) agents were assigned to investigate the 2001 anthrax attacks: code name "Amerithrax."

The investigators included a team of FBI agents and analysts tasked with the job of reviewing info bytes in the billions. For example, the bureau executed multiple search warrants and seized several computers and storage devices. A copy of the hard drives and storage devices was placed onto 2–3 stand-alone computers at the Washington Field Office (WFO). If you sat at one of the computers, you could browse a set of folders named something like the following:

- John Doe's desktop
- John Doe's laptop
- Laptop from John Doe's closet
- Girlfriend's laptop

If you opened one of those folders, you would see a folder labeled "C," and then if you opened the "C" folder, you would see a logical, recursive copy of the actual folders and files from the C: drive of the corresponding computer. This process was time-consuming and proved redundant in tracking info.

Therefore, a program called "Quincy" was employed to decode hundreds of file formats and visually (or audibly) present the data to an analyst. What is important to note is that the analyst needed only to look at the pages for each file and press one key per page: N for *not relevant,* R for *relevant,* or the space bar for *undecided.*

Still, as efficient as Quincy was, it would take the agents "hundreds of years" to manually review all the digital evidence. Therefore, it was proposed that certain "nonessential" data be reviewed programmatically using specialized tools instead of manually by agents. When this alternative was presented to the FBI Special Agent in Charge of this investigation, he responded that the director would not allow any "shortcuts" as this was the FBI's most important case.

It may have been that the FBI agent in charge did not communicate this challenge clearly enough. Or perhaps the director didn't ask for further clarification. Regardless of who was responsible for communicating or understanding the information, this unrealistic demand hindered motivation and generated the opposite of what it was meant to achieve.

Generating the "Tuna Fish Effect"

Here is what was described to me by one of the agents working on the case:

> A short time later, after the director negated the programmatic approach, I observed an agent sitting at the Quincy machines. He had stepped up the pace at which he was *reviewing* the data by pressing the N key every 1–2 seconds. This pushed the upper limits of the speed at which he could review the data accurately. A short time later, the same agent was pressing the N key about four times per second. That is, he was no longer reviewing the data—he was marking the data not relevant as quickly as he could.
>
> Later I returned and found the agent was no longer sitting in front of the computer. He had left, but he had placed a tuna can on top of the N key, which was marking countless pages of data *not relevant.*

For this article, we will refer to this behavior as the "Tuna Fish Effect": a negative organizational behavior resulting from a leadership direction based on an unrealistic demand, especially when it lacks clarification.

In essence, when leaders look for data that supports their assumptions versus acknowledging data that may contradict their assumptions, ineffective behavior follows. The leader runs the risk of misreading the situation, which directs energy away from solving the problem and instead encourages unproductive behavior that's generated by an unrealistic demand. In your mind, you are absolutely making the right decision (but at the expense of generating the wrong results).

Cybersecurity Is Complex, Layered, and Confusing to Everyone

Cybersecurity represents an idea that is so complex and layered that as author Alexander Klimburg observed in *The Darkening Web: The War for Cyberspace,* we can't even agree if the term is one word or two. As leaders, we assume that admitting there are many cyber issues we do not know or understand is a bad thing, as it weakens our position. Instead, if we reject that assumption, we expand our decision-making capabilities to better manage this complex beast.

Raising our radars to identify and manage our assumptions does not ensure we will always make the right decisions, but it does decrease the odds of our making the wrong ones. When an FBI director inferred that "no stone be unturned," he might have been saying that, "I am the boss, and nothing will get overlooked on my watch" or, perhaps, "This is pretty complex stuff, so we better cover everything since I am not sure what we should cover." These desired outcomes are understandable but assume that a.) you alone as the leader make the difference, b.) no one knows better than you do how to solve the problem, and c.) I may not be an expert in this, but I am an expert at generating results.

We have all made these assumptions as leaders and upon reflection can probably identify how they created the Tuna Fish Effect.

The purpose of this article isn't to diminish your leadership skills but rather to propose a way to strengthen them. In a world of cyber complexity, it pays to encourage both yourself and your teams to identify those beliefs on all levels, from coding to budgeting. When these beliefs are taken at face value, such as "algorithms don't make assumptions," they have the potential to thwart your best intentions by directing energies in the opposite direction than was intended.

Since most assumptions are made subconsciously, I have included a few of the key ones that might be worth reviewing and discussing with your teams.

What Is Said = What Is Being Assumed: A List Of AI And Cyber Assumptions

- I put my best people on the job = A skilled Army captain can investigate computer crimes without any computer experience
- We are keeping the enemy out = Malicious attacks come from outside the organization
- This is good code = I don't have the time to double-check its accuracy
- We have the superior technology = No one can do what we can do
- Follow the algorithm = Algorithms don't make assumptions

- Biometrics are better than passwords = Fingerprints can’t be lifted easily
- We are not a target = We are too small for anyone to care about and hack
- Cybersecurity is too complicated to understand = I’ll leave it to others to figure out
- The government will protect us = The government is technologically superior
- My ISP protects my organization = Those in charge know what they are doing

The goal of discussing these assumptions is to direct your organization to think differently while minimizing the constrained thinking that leads to nonproductive behaviors.

Perhaps a good time to do this is over lunch, but maybe you want to leave out the tuna fish.