Former FBI exec Robert Anderson Jr. dodged bullets and bombs in war zones around the world and led investigations into Edward Snowden and the cyber-attack on Sony, allegedly by North Korea. Today, he's battling cybercriminals and protecting businesses as the CEO of Cyber Defense Labs.

ENEMY AT THE GATES

story by
BEN SWANGER

portrait by
JONATHAN ZIZZO

"WAR? IS THIS AN ACT OF WAR?" ROBERT ANDERSON JR. WONDERED, AFTER BEING BRIEFED THAT THE **NORTH KOREAN** GOVERNMENT ALLEGEDLY **INFILTRATED** AND EXPOSED **SONY PICTURES** ENTERTAINMENT'S **CONFIDENTIAL** BUSINESS RECORDS. HE WAS JUST A YEAR REMOVED FROM INDICTING **EDWARD SNOWDEN** ON ACTS OF **ESPIONAGE**. AND NOW, **MORE SHIT WAS HITTING THE FAN.**

"When the guano hits the rotating oscillator," says George Newstrom, former president of NTT Data Services' federal government group, "nobody knows how to respond better than Bob Anderson."

For the first time in American history, the U.S. Intelligence community, the FBI, and private sector cyber defense companies worked together to resolve a cyberattack. At the forefront of it all was Anderson, who led more than 20,000 FBI operatives as the bureau's executive assistant director of the criminal, cyber, response, and services branch—No. 3 in the entire organization.

"They destroyed thousands and thousands of computers," Anderson says. "But in this case, Sony was a wake-up call to corporations everywhere. You always need to be evaluating your risk continuum on a cyber scale; unfortunately, I think companies have a short memory when it comes to cyber protection."

Anderson, who led the successful resolution of more than 20 spy cases during his FBI tenure from 1995 to 2016, is now erecting protective walls around businesses across America as chairman and CEO of Cyber Defense Labs, a Dallas-based private cybersecurity company formed in 2012. When Anderson joined in 2019, his first meeting with the team—around two folding tables—included the company's entire staff of seven; three years later, the operation has a clientele of *Fortune 100* companies, and Anderson is not afraid to boast about its potential.

"I want to build this into the best cyber company in the history of the United States," he says. "Some people think I think too big—but not me. If you're not thinking big, you're never even going to break even."

Anderson has always had big ambitions to lead an elite group of people, according to those who know him. It all started, though, in lowly horse stables operated by his father in Wilmington, Delaware.

A WORLD WAR II veteran who later worked in construction, Anderson's father oversaw a stable of harness racing horses. Anderson worked there every weekend and summer, cleaning stalls, carrying water buckets, and walking horses to a blacksmith shop. In that time, Anderson says he learned many lessons from his father, many of which he shrugged off at the time, but now as a chief executive has come to fully appreciate.

"Now, I think, 'Oh, my dad did know what was right,'" Anderson says. "I see many people fail because they don't listen to the men and women around them. Leadership comes with a responsibility to listen."

After graduating from the Delaware State Police Academy in 1988, Anderson finally found a sense of belonging—and what he believed was his calling. As a 21-year-old trooper, he assumed he had all the answers, overlooking lessons his father tried to teach him. His first opportunity to shine came just weeks after getting his badge.

Anderson was pumping gas into his squad car when a radio call reported an active robbery in progress at the Dunkin' Donuts in town, about 350 feet away. Anderson stopped pumping gas and rushed over to the store, but the culprits had already hurried off. He took down information from the victims, began to dial up an all-points bulletin, and that is when his sergeant arrived on the scene.

During his time in law enforcement, Anderson was cross-trained as a nationally registered paramedic (top right) and pilot.

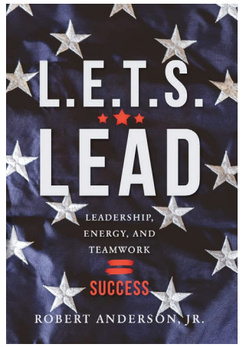
Anderson received the Presidential Rank Award, the U.S.'s highest honor presented to senior government executives.

But when Anderson's higher-up arrived, the crisis immediately changed. Over the dispatch, Anderson heard, "400 gallons of leaking gas coming from a gas station parking lot."

Several fire trucks passed by. He and his sergeant peeked around the side of Anderson's car. There they saw the gas nozzle, hose, and dispenser severed from the pump. He thought it was the end of his career. Although he was disciplined, he kept his job. Anderson says that correction propelled the rest of his trooper career. He went on to work cases of domestic violence, rape, homicide, robbery, and fatal car accidents, and eventually won Delaware State Trooper of the Year in 1990 after running into a burning home to try to save a family.

Eight-and-a-half years into being an officer, Anderson was driving down a road in Delaware, when he was pulled over by an FBI official who had previously worked with Anderson. "He knew exactly who I was, and he handed me an application and said, 'You need to be an FBI agent.'" Anderson was hesitant about the idea but sent in an application anyway. "The FBI was never some bright shining star for me," he says. Four months later, he was in the FBI Academy.

"Every one of my classmates was either a lawyer, a doctor, an engineer, a NASA veteran, or some other higher stature, and I was a state cop," he says. "I did not fit in." Anderson made it through training and picked up his first assignment in the nation's capital in the mid-1990s. He worked in narcotics and violent crime at the Washington Metropolitan Field Office as part of a major narcotics squad. At the time, Anderson says, it was considered the most dangerous field office in America.



HE QUICKLY joined the Washington Metropolitan SWAT Team—one of the most active SWAT units within the FBI, Anderson says. He later tried out and was admitted onto the FBI's Hostage Rescue Team—where he deployed to more than 20 countries, including war zones in Kosovo, Serbia, and Pakistan. He was constantly dodging bullets and bombs and broke a total of 12 bones. During his tenure on the hostage rescue team, Anderson was involved in six rescues within the continental U.S. where all hostages were rescued successfully.

But Anderson's most frightening moment, he says, came in what should have been a routine wintertime training exercise. His assault team was fast-roping out of a helicopter and onto a moving boat over the Potomac River below. "I had already been to Kosovo twice, and I chased Eric Rudolph (the Olympic Park bomber) around the woods for months—I'm a pretty seasoned guy, right? Well, I had a bad feeling about this exercise, and I voiced that," Anderson says. He was the No. 1 guy on the team, making him the first in line.

A team member on the boat held on to the rope while Anderson descended, connected only by his hands. Not even halfway down, the boat captain slipped on the throttle, and the boat lost pace with the helicopter. The sudden movement catapulted Anderson, who had 70 pounds of gear strapped to him, into the sky. He desperately clung to the rope, moving at about 17 miles per hour, dangling upside down between a freezing river and helicopter blades. "I'm going to die," Anderson remembers thinking. "I'm going to fall off this rope. There's no way I'm making it out."

After what seemed like a lifetime, the boat was steadied, and Anderson got close enough to where he could land in the boat. "The rope was cut, and no one else went down," he says. "Our leader came up to me and said I was right. That was a big deal for me. I still don't know how I held on. Fear will do a lot for a person."

In 2001, Anderson was promoted to FBI headquarters and worked as a supervisory special agent for the counterintelligence division. Along with thousands of others, he investigated the 9/11 attacks. Afterward, a new form of assault on U.S. soil began to take off: cyberattacks. In 2008, Anderson was promoted to chief of the counterespionage section in the counterintelligence division at FBI HQ.

Working alongside Anderson as his assistant director was Randy Coleman, a now corporate security exec. "I became an expert in cybersecurity because of Bob," Coleman says. Together, the two worked on hundreds of investigations. But the one that sticks out the most is Edward Snowden—who stole 1.7 million classified documents from the NSA in 2013.

"Bob was under immense pressure from all ends of Pennsylvania Avenue to solve this case," Coleman says. "They wanted a solution, and they wanted it right away."

Anderson and his team worked on the matter 24 hours a day to deliver quick results. "Bob demanded everything from us," Coleman says. "That's just the type of leader he is. He demands the best but also inspires those around him to be the best."

The situation called for an all-out effort. "What Snowden did was the greatest national security breach in the history of the U.S.," Anderson says. "He was the quickest individual in my entire career indicted for espionage. It took five days to convict him on multiple counts."

For 90 days following the verdict, Anderson was in charge of briefing FBI, White House, and Department of Justice officials on the status of the case. Snowden had fled America and found refuge in Russia. Once there, the U.S. government was never able to—and has never been able to—get their hands on him. Despite it all, Anderson maintains one thing: "Snowden, in my opinion, is a horrible hacker."

$1 TRILLION. That is the size of the cybercrime industry, according to Anderson. "There is not another crime on earth that evolves as quickly as cyber-attacks," he says. "If you're looking at the precedent from two years ago, you're never going to detect anything. I'm extremely critical of private-sector companies and our government because they don't understand this bell curve is not tapering off anytime soon."

Countless companies have experienced major breaches in the past year or so, including an attack on Microsoft that harmed more than 30,000 U.S. businesses and government agencies. Using a singular password, hackers also stormed Colonial Pipeline with a ransomware attack that sparked fuel shortages across America. Locally, Neiman Marcus discovered a breach that revealed payment data and other personal information for 4.6 million shoppers. And so much more.

Anderson served as a member of the FBI Hostage Rescue Team. He deployed to more than 20 countries and war zones.

FIRST PERSON P.O.V.

This past March, Robert Anderson published his first book, *L.E.T.S. Lead.* It details significant career moments, ranging from the time he ran into a burning building to try to save a family to office scuffles at FBI HQ. "Bob has never not delivered on something," says Randy Coleman, retired FBI executive assistant director. "Fifteen years ago, he told me he was going to write a book. He always kept a journal and would write little bubble notes down, and I'll be damned, he did it." Cyber Defense Labs board member George Newstrom sees similarities to a Dallas business icon in Anderson, who dedicated the book to his son, Dr. Robert Joseph Anderson. "Much like I used to see Ross Perot's grandkids in his office during the workday, Bob functions the same way—as a family man."

With Cyber Defense Labs, Anderson is helping executives act before a breach leads to a catastrophe. Newstrom, the former NTT Data Services exec and current Cyber Defense Labs board member, does not doubt that Anderson will achieve his mission. "There's no one more qualified than Bob to build this company," he says. "I worked with Ross Perot Sr. for 28 years, and everything I saw in Ross is everything I see in Bob. Bob Anderson is the next Ross Perot."

When Anderson joined Cyber Defense Labs three years after retiring from the FBI, his initial aim was to help small and midsize businesses prevent cyber-attacks. "We thought that would be our avenue," he says. "But now, we are working with multiple *Fortune 100* companies—these are global, $60 billion companies we're helping. And now, the key to gaining market share across the country will be to get into the cyber hubs of D.C., New York, Chicago, and Atlanta—this is just the beginning."

Anderson has built a team of 70 employees, including experts who have experience in the private sector, government, and law enforcement. Cybersecurity behemoths like Mandiant, Trellix, and CrowdStrike scale by offering a singular cyber tech solution, Anderson says; his company aims to fill a niche through risk assessments and advisory services—advanced technical services such as penetrating testing, vulnerability assessments, configuration reviews—and managed security services.

"Cyber companies come into corporations and just talk about a cyber plan," Anderson says. "They then give them a PowerPoint that doesn't do crap. I don't do that. I want to come into the partner's corporation and talk about them, talk about their business, sit down at dinner. Companies purchase $10 million worth of protection, and it's not worth anything because they have no idea where they're at risk without a holistic examination. That's what we do; we take a typically $200,000 cyber protection package and we do it for $50,000 because we look at companies as family—as valuable American infrastructure."

The strategy is working. In 2021, the privately held Cyber Defense Labs reported revenue growth of 485 percent, year over year. At mid-year 2022, its revenue is 70 percent ahead of what it generated at the same point last year. For 2023, Anderson is projecting growth of 33 percent. As things currently stand, revenue earned in its cyber-managed security services unit has grown 175 percent per client in the past 12 months.

"I've seen over the years, especially in the FBI running very large scale, complicated, serious things—whether they're spies or terrorists or hostage rescue missions—you must have a vision of how things are going to end," Andersons says. For Cyber Defense Labs, though, the end is nowhere in sight. In fact, it's just the beginning. But, as he has done ever since he was a child, Anderson is thinking big. "Frankly, we're beating the larger cyber firms because our people have been there, done that when it comes to large-scale cyber protection," he says. "We're aiming to grow our market share by 50 percent this year in Texas, then double next year across the country … then we really plan on monopolizing this." D

OPENER BY **MARCOS OSORIO**. ICONS: **SHUTTERSTOCK**; ALL OTHERS COURTESY OF **ROBERT ANDERSON**

FIVE CYBER SECURITY TIPS FOR EXECUTIVES

U.S. companies experience nearly 30,000 cyber-attacks each day, Anderson says, and executives should be on top of protection not monthly, not weekly, but daily. Here are his tips for remaining vigilant:

ONE

DISCUSSIONS

"Make cybersecurity a daily conversation. All it takes is one person who's having an off day to click or download one little file and it turn into a catastrophic event for your company."

TWO

AWARENESS

"Know the enemy. Hackers think what they're doing is right. They are all narcissists, and they are typically always after monetary gain—with a few exceptions, like the Sony case."

THREE

VIGILANCE

"Apply protection liberally. What a CEO or CFO believes to be the biggest risk in their company is not the same. So, identify each risk and overlay protection over every single one."

FOUR

TRAINING

"Train your people. Do they know what the instant response plan is? Do they back up their data? Is your data segmented—can it be found on one central system, or is it broken down into segments to increase security?"

FIVE

RESILIENCE

"Realize that you're never safe. Cybercriminals don't give up. Just because you have defeated them once doesn't mean they are gone. You must be resilient and question how they are going to attack you next."