

## INTRODUCTION

As we approach the 20<sup>th</sup> anniversary of September 11, 2001, we thought a different and more far-reaching use of the SIMS Software Blog would be fitting. As shared with our contributor Tom Langer, we collected personal reflections on 9/11 from current and former leaders in the security profession. As their professional affiliations show, many of our participants also had extensive careers in government security.

We asked each leader the same three questions regarding their lasting memories from that day and how those experiences shaped their careers, how the security profession has adjusted to the changing landscape, and what advice they would have given their younger selves in preparing to take leadership roles.

The result is a touching collection of deeply personal vignettes, each capturing our contributors' unique experiences in their own words. Our job was to get out of the way, let them reflect, and capture those reflections for this special compilation. We hope you find this particular blog as meaningful as we do, as we remember and pay tribute to all those we lost as a result of September 11, 2001.

## CONTRIBUTORS

SIMS Software is honored to have the following 10 security leaders sharing their personal stories and insights in this special blog.

- **Ed Halibozek**, Vice President of Security (ret.), Northrop Grumman
- **Rick Lawhorn**, Former Director, Industrial Security Field Operations, Defense Security Service
- **Mike Londregan**, Chief Security Officer, Peraton; Former Director of Security and Insider Risk, Defense Intelligence Agency. On 9/11/2001, Mr. Londregan was serving as the Continuity of Operations and Disaster Recovery Program Manager for the Defense Intelligence Agency. His office was located in the "A" ring, second corridor, in the Pentagon.
- **Jeffrey Mazanec**, Chief Security Officer, General Dynamics; former Deputy Assistant Director, FBI
- **Mary Rose McCaffrey**, Vice President of Security, Northrop Grumman. On 9/11/2001, Ms. McCaffrey was working for the CIA and assigned to the Department of the Navy.
- **Mike McGinty**, Group Security Director, BAE Systems (1994-2013); Wing Commander (ret.), UK Royal Air Force Security Branch
- **Charles Phalen**, Former Acting Director, Defense Counterintelligence and Security Agency; Former Director, National Background Investigation Bureau; Former Vice President of Security, Northrop Grumman
- **Dan Schlehr**, Vice President, Global Security Services (ret.), Raytheon Company

- **Michelle J. Sutphin**, ISP, Vice President and Chief Security Officer, SAIC; Chairperson of the Security and Counterintelligence Division of NDIA; Former NISPPAC Spokesperson
- **Bob Trono**, Chief Security Officer, Lockheed Martin

## VIGNETTES

**Question #1:** This September 11, we will pause and remember the magnitude of that day 20 years ago. What are your lasting memories from September 11, 2001, and how did that experience shape or dictate your career or career choices?

**Ed Halibozek:** One lasting memory I have is how surprised we were that terrorists would use multiple commercial aircraft to commit such a devastating act of terror on U.S. soil. Although we had recent experience with acts of terror committed within the U.S. (the 1993 World Trade Center truck bombing and the 1995 Oklahoma City truck bombing), the use of commercial aircraft in a coordinated attack was new. This event opened our eyes to the need to better assess and understand the threats to, and vulnerabilities of, our domestic assets against acts of terror. It also drove us to improve our contingency planning processes beyond preparation for acts of nature to include manmade events - in particular, acts of terror.

After the events of September 11<sup>th</sup>, emergency preparedness and contingency planning were given much greater emphasis with C-suite executive support. Moreover, the greater security community, which I believe already worked well together, seemed to become even more collaborative on matters of asset protection.

**Rick Lawhorn:** I believe my most lasting memory was watching the World Trade Center buildings on fire on TV at the office, then looking out the window and seeing the smoke coming from the Pentagon. This was before it was announced on the news that a plane had hit there as well (I was working in Alexandria, VA at the time). At that point, my thoughts turned to the friends, co-workers, and colleagues I had at the Pentagon. There were also numerous rumors of bombs exploding throughout Washington, DC, to include the State Department where my sister worked. Finally, I remember getting home that day and having neighbors going door to door checking on everyone, since there were many military personnel that lived in our neighborhood.

I can't say that 9/11 had a tremendous impact on later career choices or my career, other than to make it even more clear to me that our job at DSS was to support the warfighter in any way we could. For us, that meant stepping up our oversight efforts in cleared defense industry and finding creative ways to get companies to work securely to build the weapons systems, materials and hardware the military needed in its war efforts. At the time 9/11 occurred, we in DSS were already attempting to refocus on core mission activities such as security reviews, accrediting classified computer systems, and expeditiously processing new facility security clearances (FCL) after failed reinvention initiatives in the 1990s. I would say 9/11 helped to clarify and even expedite those efforts.

**Mike Londregan:**

- Leaving the house that morning and realizing halfway to work that I left my cell phone at home.
- The ever so slight shake of the Pentagon when the plane impacted. It speaks volumes to the building's strength literally and figuratively.
- The orderly and calm evacuation out of corridor #2 into south parking.
- The amount of first responders who arrived on scene in such a short window of time. Never take these folks for granted.
- The ground-shaking explosion of the airplane's fuel bladders and the resultant black smoke that literally blocked out the sun as we walked into south parking.
- The inability to effectively coordinate and execute established COOP/DR plans due to the cell phone outage and bridges over the rivers in gridlock.
- The bewilderment of people in the parking lot not knowing what happened, and the only source of info was WTOP News.
- Running into the DIA CIO in south parking who was in shock and babbling about how the plane went right over his head before disappearing into the Pentagon.
- Finally getting through to my wife at 11:45 using a colleague's phone. Given the jammed networks, all I had time for was, "I'm out, I am alive and safe. I will see you when I see you." Click.
- The generosity of hotels and Costco in Pentagon City, who brought out pallets on forklifts loaded with water, towels, food, etc.
- Trying to conduct accountability of personnel from just a phone roster in the business center of a Pentagon City hotel.
- The helpless feeling when the DIA Chief of Staff told us to go home at 1700 on 9/11 after we faxed the list of 19 unaccounted DIA employees into the National Command Center inside the Pentagon, where the Director of DIA was working.
- A long, solemn metro rail and metro bus ride out to Vienna. In an adrenaline-drained confused state, I recall there being a few people per car and only one other person on the bus.
- Getting home at 7:30 p.m. and hugging my wife and two daughters.
- The legal pad of 70+ names of family and friends who called my wife during the day asking about me. You never know the power of your support network until you truly need it. Never take it for granted.
- Turning off the news and turning on some music. The song that came on was U2's "Walk On" from their album *All That You Can't Leave Behind*. Look up the lyrics and it will make sense.
- The anxiousness to get back to work at 4 a.m. the next day.
- Walking over to the impact zone on 9/12 and feeling professional anger at my own community's inability and unwillingness to share, collaborate, and integrate intelligence.
- Being 50 feet away from President Bush when he pulled up to the "open wound" on 9/12 to be with the rescue and recovery workers. This was the iconic moment when first

responders unfurled the large flag that stayed draped over the Pentagon until the one-year anniversary.

- Attending six funerals for colleagues in the fall of 2001.
- Holding onto the 9:34 a.m. email that our comptroller Chuck sent me as a follow-up to our phone call a few minutes before. Chuck was killed at impact at 9:37 a.m.
- I committed to doing my part to be a collaborative contributor between IC brethren.
- Deeper commitment to closing the information gap between national-level intelligence and federal, state, and local law enforcement.
- I purposefully went to the ODNI at standup in 2004 to help with intelligence integration, and in 2008 served as the deputy for federal, state, and local law enforcement partnerships. The purpose of the office was to close the aforementioned gap/void. Extremely rewarding.

**Jeffrey Mazanec:** America was changed forever on that day, and so was I. In my role as a career FBI agent, who was running a Joint Terrorism Task Force (JTTF) and actively working to prevent a major act of terrorism against the U.S. and its citizens running up to 9/11/01, I was tremendously impacted by the attack. I kept saying to myself over and over that this just could not have happened. The events of that day were seismic, bigger-than-life, certainly life-altering. I was part of the response in Washington D.C., and we worked nonstop for many months to ensure the attack was fully investigated and that there would be no follow-on attacks on U.S. soil. And we did in fact prevent any further attacks, because of the dedication, hard work, collaboration, information sharing, and personal commitment to our national security after that fateful day.

**Mary Rose McCaffrey:** 9/11: Lasting memories, clear sky, eerie noise, smoke plume, answering machine blown up. Outside of DC, people had no idea of the spatial distance of events in DC. The reality of “not knowing” the true extent of the events of the day put everything into perspective of the history that was about to unfold. Security changed dramatically overnight. Priorities from tradition changed overnight. Like every catastrophe, Monday morning quarterbacks were in overdrive: how could this happen and why didn’t we see it? War footing changed dramatically.

**Mike McGinty:** Like many others, I can remember exactly where I was and who I was with when I was alerted to the 9/11 attacks. The images of the Twin Towers on the TV screen in the office created a true sense of immediacy around what was happening on the other side of the Atlantic. The event was of a magnitude that rendered it beyond shocking, and I think its sheer scale and suddenness, alongside the common interests that many of us in the UK share with our U.S. friends, colleagues, and counterparts, almost gave the sense this was happening on home soil. I’m guessing that most of us shared feelings of dismay and anger, but we can also recall the calm and determined professionalism of so many of our colleagues in dealing with the immediate aftermath and the adjustments that were needed in the ensuing weeks and months.

Just prior to and following 9/11, my own company was taking on an increasingly international flavour. That brought about the need, not least among our own security professionals, to learn about the many different ways in which people choose to solve the same problem, and how to adjust and adapt as necessary to different perceptions and methods. This is of course a two-way street.

I'm pretty certain that the major coming together of ideas, and the exponential increase in what I will call the International Security Contact Base that came about as a direct response to 9/11, caused a significant shift in my own professional priorities and in those of countless colleagues and counterparts in the security profession globally. Looking at how other folks do this stuff became a priority rather than an add-on, and this was a huge plus in taking things forward in an increasingly international and complex professional environment.

**Charles Phalen:** Across Washington, DC, police officers at the White House, Capitol, CIA, Federal Protective Service, and other federal agencies moved quickly to control, to protect, and to bring calm to a volatile situation. Sitting at my Security Operations center at the CIA and moving throughout our headquarters compound, I marveled at the unflinching professionalism of our officers in the face of almost certain knowledge that other aircraft were loose in the skies.

This scene of courage repeated itself at federal facilities around the city and across the country. And it continued as together we dealt with countless threats and scares, including the Anthrax attacks which began several weeks later. The sense of fear was palpable in the city, but the professionalism of these officers played a critical role in keeping things under control.

Moving closer to the present: Earlier this week, all the neighborhood kids were gathered on the street corner, waiting to jump on the bus and head off to the first day of the school year. This sight brought up a vivid and recurring memory from 20 years ago. When I got back to my neighborhood very late in the evening on September 11th, I came upon a group of adults and children gathered on that same street corner, with candles burning on the curb, all trying to comfort each other. The next morning, the school kids were there, waiting for the bus amidst all those stains. The marks remained visible on the curb and sidewalk for most of the next two decades until some road repair finally covered it last year. The stains are gone and none of the kids at the stop today were around in 2001, but that corner and these kids still serve as a reminder to me.

**Dan Schlehr:** I remember 9/11 like it was yesterday. I was sitting at my desk, the TV in my office on, waiting to watch an interview with Jack Welch, the CEO of General Electric. I had worked closely with Jack during my seven years with GE. It was first reported that a small plane had crashed into one of the Twin Towers. When the first footage aired, I knew it was not a small plane and I feared the worst. Shortly thereafter, the South Tower was struck by another aircraft. I remember shouting to my security staff to lock down Raytheon's global headquarters. I then called my leadership team across the company to increase our security posture. A few

minutes later, I was called by Raytheon's CEO, Dan Burnham. Dan asked if any of our employees were on those planes. Before we could begin our research, the Pentagon was struck. Some fifteen minutes later, the South Tower collapsed. Ten minutes later, brave passengers brought down the hijacked plane in Shanksville, Pennsylvania. Twenty minutes later, the North Tower fell. Those 105 minutes changed our world forever.

We were attempting to check with the airlines to determine if we had employees on those flights, but their systems appeared to be shut down by law enforcement. Fortunately, we had a redundant paper reservation system, but the process would take time.

I am from Buffalo, NY, and many of my college friends lived and worked in NYC at the time, so my mind was racing. I received a call from my brother, who told me his wife's sister worked in the Towers and was missing, and asked if could help. I called my college roommate who was a Captain in the NYPD at the time, but was unable to reach him. I felt helpless.

After checking and rechecking our records, we determined four Raytheon employees were on American Airlines flight 11.

I spent a great deal of time in our CEO's office that fateful day. We discussed how the company should respond and how we would review and possibly reevaluate our security program. After 18 hours in the office, I came home to my wife and 10-month-old son. My wife also attended college in New York. She too had missing friends.

That horrible day made me resolute to contribute to our nation's security. I had started my career with the Diplomatic Security Service as a Special Agent, and after seven years, I left federal service for the private sector. As previously mentioned, I started my private sector career with GE. After GE, I worked for Philip Morris before starting with Raytheon in July of 1999. I was ambitious and willing to leave for the next opportunity. 9/11 changed my mindset. I knew I would remain at Raytheon until my retirement.

**Michelle J. Sutphin:** On September 11<sup>th</sup>, I was working as a HR Coordinator in my very first job out of college. I was newly married and had just spent my honeymoon in New York that June, so the energy of the city was still fresh in my mind. I remember walking into my office building on that clear beautiful day and seeing my friend standing at the receptionist desk. We had just installed large flat-panel TVs in the lobby and he was eying CNN with intensity. I remember looking at him and asking "What's up?"

He responded, "A plane just hit the World Trade Center." I remember thinking it was unfortunate and went to my desk to start work. Right around that time, emails started shooting around the office that the building was on fire. Realizing how large of a building this was, I decided to go into our auditorium where the news was being broadcast on a large screen. I remember standing there with about 15 other people, watching the smoke, watching live when the second plane hit. All of our stomachs collectively dropped as we now understood this

was intentional. Shortly after, we got word about the Pentagon and that's when my team got to work to accounting for all of our employees working there. One of them called from her cell phone to tell us she was driving to work when she saw the plane fly over her head before it hit. As soon as the last plane crashed in Pennsylvania, I remember bursting into tears, walking into my boss' office and saying, "Can I please go home?" He looked at me and said, "Michelle, you do whatever you think is best."

My apartment at the time was right next to Dulles International Airport. I was terrified to be anywhere near an airport at that time, so I somehow managed to get through an hour of busy signals and told my husband to meet me at my parent's house in Haymarket. The rest of the night was spent glued to the television, listening to the roar of the fighter jets flying overhead as they patrolled the airspace.

The next morning, the entire country woke up to a new reality and a new world. I remember it was impossible to find flags. They were sold out everywhere so I spent my nights making them out of construction paper and hanging them on office doors throughout our building.

It's an interesting question, asking me how this day shaped my career. Because I was so new in industry, I really learned everything I know today post-9/11. I didn't enter the security profession until 2003, so I spent most of my time learning and absorbing from mentors and most everyone on this blog to figure out what I should and should not be doing.

**Bob Trono:** I remember the day clearly. I was an Assistant United States Attorney in Richmond, Virginia. That morning I was handling an arraignment on a drug case. I walked across the hallway in the U.S. Marshal's Office and watched the second plane hit the tower. As a personal consequence of that day, I ended up serving at Main Justice and the U.S. Marshals Service, which led to my role at Lockheed Martin.

**Question #2: The defense, intelligence and law enforcement fields underwent several transformations since 2001 that impacted the security profession. What is your assessment of how well the security profession has adjusted to the changing landscape, and are we better positioned against existing and emerging threats?**

**Ed Halibozek:** Initially, I do believe the security community made positive adjustments to enhance protection of assets against a broader spectrum of threats. However, as time passes, corporate memories are short. The early emphasis placed on enhanced security protections and contingency planning begins to wane along with the willingness to incur the costs of those measures. Memories are short and priorities change. The challenge security professionals have, and may always have, is to ensure they quantitatively demonstrate the value their security program brings to the organization.

**Rick Lawhorn:** I think for the most part, the security profession has done a good job at adjusting to the changing landscape, and I definitely believe we are better positioned than we were 10 to

20 years ago. There has been a great deal of progress in terms of incorporating threat into the implementation of security countermeasures through better information sharing between government and industry. I also believe there is a much greater understanding of the threat, especially as it relates to cyber and other complex security matters. There is still a lot of work to do however.

To begin, in relation to cyber (and other threats), the threat always seems to be ahead of the countermeasures applied. In short, our understanding of the threat and our ability to respond tends to lag behind – mainly because we are constantly observing what our adversaries are doing and it’s constantly growing more complicated and diverse. Often, we are one to two steps behind.

Next, the security policy formulation, though better the last two to three years, still lags behind the threat, making it difficult for security managers to apply effective countermeasures. It’s difficult to sell senior management on costly new security countermeasures that aren’t mandated by contract or policy. I do believe we are getting better at this, but it’s such a complicated and bureaucratic process that it takes way too long to get addressed.

Finally, there still needs to be a much closer relationship in government between the security and acquisition communities. Until we get to a point where security countermeasures are considered, funded, and applied in the initial acquisition process, security for the most sensitive (non-SAP) programs will always be underfunded. In other words, if there are threats to specific priority DoD acquisition programs that aren’t SAP, they need to be identified so the bid process will account for those costs at the front end.

**Mike Londregan:**

- 9/11 compelled a huge transformation in collection and analysis, in order to be more predictive and proactive. This in turn compelled security to pivot and enable new missions. I feel we did so with agility and creativity.
- We constantly reminded each other that 9/11 was a failure of imagination and lack of proactive thinking on the security community’s part.
- No one questioned the “asks” or “needs” in the immediate years following which allowed for some overkill in our approach to risk mitigation.
- The emotion and rawness of the event created a permissive environment for unquestioned spending.
- As time and distance got greater, the pressure grew on security leaders to develop risk-based solutions and develop a sound, reasonable value proposition for the mitigations. 9/11 became less of a rationale.
- The rise of the insider risk supplanted the threat to the homeland for me as an IC security director. The security community again pivoted to a different threat while ensuring it wasn’t at the expense of protecting “the perimeter.”



- Our security community seems to adjust very well to changing risk landscapes and varying threat vectors on a simultaneous basis. We underestimate how good our community is at managing and mitigating the multitude of threats.
- Seminal events like 9/11, Snowden, etc. create pathways forward and soon we have multiple paths that run parallel and some overlap. The key is to remember that we are on those paths together and we must always ask.....“Who else needs to know?”

**Jeffrey Mazanec:** 9/11 was a transforming event, bigger than any I’ve known in my lifetime. The 9/11 attacks forever changed the way law enforcement and intelligence agencies do their work. The same can be said of private security professionals and our industry. Today, we work to anticipate the threat, set up layers of defense, and use all means to mitigate it. Prevention, not active response, is now the name of the game, post-9/11. We are now focused on very significant tool sets in the security realm, including: the intelligence cycle, connecting the dots with analysis, information sharing, threat identification and mitigation, the prioritization of threats, leveraging our resources, and threat hunting not mere compliance. I think the security profession has adjusted slowly to the shift from compliance to threat hunting, mostly because of the ingrained requirements of the Cold War. One of the transformational aspects of the 9/11 attacks was to move the U.S. from a long-term Cold War approach to a more agile, quick counterterrorism response. It took 10 years or more, but significant progress was made, especially in the industries that support the national security and defense missions. Even though the shift toward counterterrorism blinded us temporarily to hostile-nation espionage, 20 years later we are capable of working all threat areas with a very versatile set of tools and an extremely talented workforce.

**Mary Rose McCaffrey:** I think security adjusted well in the first decade following 9/11, pivoting to GWOT, but they also focused singularly, while neglecting other threats. Personnel were given significant training and focus on terrorism. In some ways we are more agile, but are we better positioned against emerging threats? I am not 100% convinced the answer is yes. Security professionals must balance tactical activities with strategy to enable delivery. Security professional development is inconsistent, sometimes dependent on the priority of the moment. We pivot to the issue of the day. Security, depending on alignment in an organization, varies in its ability to influence, partner, and add value to an organization. Relationships and partnerships have enabled security success since 9/11.

**Mike McGinty:** I go back long enough in security management of one sort or another to remember when things were a lot easier for the security professional than they are today. Or maybe I just wasn’t getting it!

I have been out of the game for several years now but still take more than a passing interest, although obviously not from an insider’s perspective. Security issues – whether it’s terrorism, crime or cyber-related (and how can we now separate those categories?) - are not only becoming more frequent, but also increasingly complicated. And the rate of change is quickening.

Government-sponsored activities have undoubtedly changed in developed nations in response to the altering security landscape, but so has the response of the security profession. I see the profession as having become increasingly agile and more “joined up” both within itself and with other vested interests including the official agencies. The relative attractiveness of security as a mainstream career compared with other sectors has undoubtedly grown in recent years, with the corollary that the profession’s combined intellectual firepower has also blossomed. Additionally, much-increased public interest in matters of security, in no small measure spurred by the events of 9/11, has elevated the profile of the security profession and caused a move to greater openness, accountability, and all the benefits that brings. As much as armchair critics can be irritating, even they have their uses!

**Charles Phalen:** For me, it is about expanding the focus of a security/protection portfolio. Over time, much of the security philosophy has been to prevent a bad event through deterrence or denial. While the need to anticipate and plan for the event to happen has not been ignored, there needs to be more done on event anticipation and response. Part of this is the imperative to share threat information. This takes on greater emphasis after a difficult event, such as the 9/11 attacks.

The information flow has certainly improved in the past two decades and we can document instances where such warnings have thwarted an attack, but we cannot rely completely on the hope of advanced warning as a strategy because the information is typically neither timely nor precise. There is still a need to presume that an attack will occur with no warning and to plan the response accordingly. In short, we need to share information on current and predictable attack tactics, quickly advise prospective targets of any inkling of an actual event in the works, and build our countermeasures and response scenario with the assumption that the event will occur – and without any meaningful warning. Lastly, two decades have helped articulate that the playing field is ever widening. Terrorism, cyber, insiders, facility compromises, and just plain and simple mistakes all contribute to the challenge. While we are better positioned today than we were, we must continue to look into the future to figure out the next challenges, all while realizing that the old challenges don’t just go away.

**Dan Schlehr:**

My peers within the defense industrial base and I formed a friendship and a bond that is difficult to describe. We worked closely with both law enforcement and the intelligence community, improving communication and sharing threat information. There continues to be room for improvement.

The security profession has adapted to new threats; however, we have been slow. In most cases we are reactive, not proactive. In my experience, funding from the C-Suite does not flow until there is a major event that impacts the bottom line or there is an unflattering event mentioned in the media. I believe we are better positioned now versus 20 years ago, however

we as a profession must continue to fight for resources. Memories are short and we must never forget.

**Michelle J. Sutphin:**

An image I remember quite vividly from 9/11 footage are the papers floating from the sky from all of the filing cabinets – like confetti. We were a hard copy world back then. Since that time, businesses have embraced scanners and servers and cloud environments with redundant failover sites. Security went from guns, gates and guards begging for funding to cyber, cyber, cyber with a significantly larger budget. We also went from being very specialized professionals to having to know and learn many aspects of security just to keep up with the changing environment. Your average FSO these days needs to be able to comprehend physical, personnel, classification management, IT infrastructure, cyber, CI, crisis management, program and industrial security all at once. We no longer have the luxury of being specialists, and yet the government does. So one of us must interact with a dozen of them, learning personalities and policies on the fly.

Through all of this, I think what security professionals have learned the most is *how* to adjust. The only constant in our profession is change and we have gotten quite adept at learning how to shift course quickly. And as horrific and hard as 9/11 was, I honestly feel the biggest impact to our profession was and is COVID. Lots of us had to build long-term crisis teams on the fly and learn how to work with laws and regulations that changed daily. Instead of securing thousands of facilities, we are having to teach people how to secure electronic information from hundreds of thousands of homes. Discussions regarding classified IT from the home are actually now a reality. So I guess in a way, you could say 9/11 laid the framework to shift us from a physical reality to a virtual reality and armed us with bigger budgets and more staff -- but COVID sealed the deal.

Are we *better* positioned against existing and emerging threats? I say no. I think we are just now coming to the realization that we are combating different kinds of threats and we are figuring out ways in which to solve these issues that have stemmed from a “new normal.” And I think in terms of long-term planning, we are realizing that we need to now plan for the unexpected.

**Bob Trono:**

The entire security infrastructure changed dramatically and permanently from that day forward. I think that over time, as we better understood the risks and the best security responses, we adjusted appropriately. There was a lot thrown at our community at once and it took a lot of time, blood, sweat and tears to get where we are today.

**Question #3: Given the importance the 9/11 Commission put on leadership and collaboration, what advice do you wish you could have given your younger self as you prepared to take your first leadership role?**

**Ed Halibozek:** Securing organizational assets is not the exclusive responsibility of the security organization. The effectiveness of an assets protection program involves the entire organization. That is best accomplished with an enlightened and cooperative management team and a receptive rank and file.

The advice I'd give to my younger self is to actively and diligently work with the organization's executive team to develop their committed support to the entire assets protection program. Furthermore, to place a greater emphasis on training and education for the rank-and-file employees to develop an organizational culture committed to protecting company assets.

**Rick Lawhorn:** I think the most important advice I would give to myself is to focus on leadership training and experiences before I became a supervisor and leader. Looking back, I had no real clear idea or philosophy on how to lead and supervise people – basically I did a lot of it by the seat of my pants using my best judgement. Instinctively, I did understand the importance of collaboration and depended a lot on my colleagues for advice and assistance. However, most of the people I relied on tended to think like me and had similar experiences. So, I would advise my younger self to seek input and help from those who thought differently than I do – in other words, get outside of my comfort zone. I realized over time that I learned as much or more from people with different ideas, experiences, etc.

I would also advise my younger self to listen better – listen to colleagues, superiors, customers, stakeholders, and most importantly, my subordinates. As my career progressed, I realized the more information I had, the better decisions I'd make. I also learned that the best decisions were the ones that the most people understood and bought into, and those things came when people felt like they had a voice.

Finally, I would advise my younger self to communicate as often and as clearly as you can. You can never communicate enough. Explain the rationale for decisions as best you can, and never stop - because in the absence of information I find that people start to make things up and often that leads an organization in the wrong direction.

Lastly, I'd advise to focus on what you can control. I spent a lot of time in my career trying to fix or influence things that in the end I couldn't control, and it led to frustration and reduced the time I had to address those things that were under my control.

**Mike Londregan:**

- Professional humility is empowering.
- Hard jobs are made easier through information sharing and collaboration.
- Establish trusted relationships and partnerships in advance of needing them.
- Know who is on the team and what they can bring to the fight.
- Held information is worthless. Shared information is powerful.

**Jeffrey Mazanec:** Leadership is the most important thing in any mission involving people. Leadership is all about making a team's mission clearer, motivating people to do better and work together, empowering their efforts, and providing the resources to finish the job well. I wish I would have understood all of those components when I was younger and just starting my first leadership role. The closer a team works together, the greater their impact. I think 9/11 taught agencies, companies, governments, neighborhoods, and countries these lessons, and I hope we will remember them.

**Mary Rose McCaffrey:** Leadership requires collaboration, which is often a result of extensive relationships, career development, mentors, advocates, along with opportunity, place and time. It is hard enough in a single organization where silos exist. Add the complexity of organizations, different mission statements, and then add the industrial partners. On a good day, it is quite a navigational adventure. I am not sure I would have given myself different advice. My personal success was taking the action and if I had to course correct, I was okay. I asked a million questions and didn't let anyone see me sweat. I took risk and was not penalized, but encouraged.

**Mike McGinty:** I would stress the benefits of developing a genuine curiosity from the get-go about how other people in a similar job do things, and why. Don't wait for something to happen that makes you look for a possible different approach - look anyway! Don't assume that the people who trained you or set your examples had all the answers. In fact, don't assume very much at all; go and find out.

Do be prepared to listen actively and do be prepared to change your mind. Good leadership includes driving change for the better; but if it's already working okay.....you know the rest! Take every opportunity to foster professional relations with people outside your environment. It is nearly always a rewarding activity. If people don't seem to think like you, there's a reason and sometimes it's a good one! You might even see examples of how definitely not to do something. Who knows until you look?

The relationships that you form will bear fruit for many years to come, and you will be immeasurably better at your job if you take the assessments of others into account. There is enormous value in sharing ideas and experience with fellow security professionals whether or not they operate in the same sector. Such exchanges can either reinforce your existing convictions or cause you to modify them. Either way they will give you added confidence to pursue what you believe is the correct course.

When you look back on your career, you might notice that some of the most useful activities you embarked upon owed their origins to something you learned outside your immediate environment.

**Charles Phalen:** Teamwork is a term that is often emphasized, but in this business, it is not always well-defined. The "security" team is one thing, but the teaming required for an effective

security program needs to permeate the organization. Some logical questions from the average person about security would be: “So, how is this my problem to solve?” and “What are you going to do about it?”

We need to get beyond basic awareness, answer those questions, and engage our constituent populations to accept some level of responsibility and participate actively in the strategy. There will never be enough budget or personnel for security to be the responsibility of only security professionals – security awareness must be embedded in the culture of our organizations.

**Dan Schlehr:** Be humble and learn from everyone. Establish your network, both in the private sector and the public sector. Establish relationships with every level of law enforcement, as well as your customers. Find a mentor or a trusted colleague, preferably outside the security field. Become a mentor to the next generation of security professionals. Finally, be generous with your time.

**Michelle J. Sutphin:** I was a manager for many years, but I truly grew into my own and became a leader when I became the Vice President of Security for the Platforms and Services Sector at BAE Systems.

There is no specific formula to being a great leader. Each respected leader has their own style and way of doing things. However, I have found that the ones I always looked up to were able to adapt themselves to each person they interacted with. You cannot treat all people the same, as all people are different. The leaders who can empathize and adapt to others while at the same time sticking to their own code of ethics in a humble way are the ones that go far.

If I could look back at that time again and give my former self some advice, it would be this: do not doubt yourself. Always listen to your gut, follow your inner voice, treat everyone with respect, and do not ever compromise your values.

**Bob Trono:** I would say, have the confidence to be more humble. You learn so much more, are more effective, more inclusive, and a better leader by acknowledging you know less than you think you do.

---

### **About the Author**

Mr. Thomas Langer has a 30-year track record as an industry security executive, including 20 years with BAE Systems, and will be periodically sharing his knowledge on crucial, relevant topics here on this Blog page. [Learn more about Thomas here.](#)