Interested in learning more about security?

SANS Institute InfoSec Reading Room

Building the Airplane in Mid-Flight: Bringing Cyber Security Structure to Special Operations Units

Special operations units, born in the fire of urgency and required to be dynamically flexible, may operate for many years without a single cyber security representative. Once hired mid-stream into such a construct, a cyber security professional can be immediately overwhelmed with the breadth of the challenge before him or her: how to overcome cultural and technical challenges to introduce a comprehensive cyber security program into the ad-hoc structure of multi-classification, multi-network, multi-agency information sy...

Building the Airplane in Mid-Flight: Bringing Cyber Security Structure to Special Operations Units

GIAC (GSEC) Gold Certification

Author: Adam Baker, abakersans@gmail.com
Advisor: Stephen Northcutt
Accepted: 20 October 2017

Abstract

Special operations units, born in the fire of urgency and required to be dynamically flexible, may operate for many years without a single cyber security representative. Once hired mid-stream into such a construct, a cyber security professional can be immediately overwhelmed with the breadth of the challenge before him or her: how to overcome cultural and technical challenges to introduce a comprehensive cyber security program into the ad-hoc structure of multi-classification, multi-network, multi-agency information systems and personnel. However, when armed with the lessons from cyber professionals from similar units who were thrown into a similar cauldron and succeeded, a newly-hired information security officer or manager *can* bring order to the unconventional chaos and ensure continued mission success. This paper will examine the experiences of cyber security professionals who overcame the challenges of securing information systems and personnel in units decidedly different from the rigid DoD structure or the corporate world. After reading, new information security professionals will have practical principles for securing their systems and soldiers, staying out of jail, and enjoying their jobs!

1. Introduction

The military is usually associated with a rigid, predictable structure. For conventional units, one Army brigade, a Navy group or an Air Force squadron looks very much like another. However, special operations units are created specifically because a unique problem or a particularly challenging set of enemies cannot be overcome or defeated by anything the Department of Defense has in its standard, predictably-organized inventory. Consequently, each special operations unit is specially designed and most are unlike anything else in the DoD arsenal. As such, "Special operations require unique modes of employment, tactics, techniques, procedures, and equipment" (Department of Defense, 2014). That uniqueness becomes the essence of the special operations unit, its reason for existence and the core of its identity. SOF (special operations forces) units are given America's most difficult problem sets and are expected to engage their missions quickly.

Because many SOF units are created and fielded very rapidly to address an immediate need, the initial priority of the unit's operators (the tactical soldiers, sailors, airmen or Marines executing the missions), unit leaders and support personnel is to get the operators trained, equipped and "into the fight" as quickly as possible. The communications infrastructure required to support operations, planning, intelligence analysis and interoperability with other forces can quickly become a dizzying collection of borrowed, ad-hoc, or home-grown systems. Because of the intense focus on engaging the problem quickly, support personnel who are not deemed immediately critical to executing the mission may not be recruited or hired for months, or even years. This delay is pointedly true when it comes to hiring cyber security personnel, whose requirements on the network can be viewed as hampering the mission's speed and flexibility.

For anyone looking to join a special operations unit in any capacity, just getting in the door is a challenge, as the recruiting and hiring process is notoriously difficult (even for non-tactical, support positions like cyber security). It can include technical proficiency tests, a psychological examination, strenuous physical fitness examinations and maintaining a fitness standard beyond that of their branch of service (Department of

the Army, 2013). It may also require a willingness to attend the Department of Defense's Survival, Evasion, Resistance and Escape (SERE) course (Department of the Army, 2013). Even for contractor personnel who may not have to meet the same grueling physical fitness standard, if they do not have significant SOF or military experience, cultural differences alone can be enough to keep many candidates from pursuing such job opportunities, or may dissuade the unit from hiring them.

When an information security professional *is* finally brought in to create a comprehensive cyber security program at a SOF unit, that person is faced with a host of daunting challenges. The mandate to secure the information environment may include thousands of users spread over separate networks with different classifications in multiple (sometimes remote) locations. This challenge is exacerbated by including networks used by unit members but managed by another enterprise headquarters element; locally-developed and administered networks; nodes from other US government agencies' networks; and foreign partner networks. The cyber security professional will have to navigate the existing relationships between local administrators and cyber officers at the enterprise headquarters, overcome many unit members' natural bias against added requirements, and understand and apply US government, DoD, intelligence community (IC), and service-specific information security regulations.

This paper will explore the common challenges, pitfalls, and successes of the cyber security professionals who oversee information security at the most elite special operations units in the United States military. Their perspectives were gleaned during interviews with the author. Due to operational and personal security requirements, these professionals are represented with pseudonyms, and their units identified only by the appropriate branch of service and description. These findings will serve as a road map for success for the newly-hired cyber security professional, shorten the learning curve, and keep that person out of trouble, out of jail, and more fulfilled and effective at work!

Adam Baker, abakersans@gmail.com

2. Overcoming Common Early Challenges

2.1. Perception meets reality

2.1.1. Pre-conceived notions

Even with their operations shrouded in secrecy, SOF units have gained a reputation inside and outside the military for expecting the highest levels of performance, strictest operational standards and a low tolerance for mistakes. This preconception leads aspiring SOF unit cyber security professionals to believe the information security situation will be much more robust upon arrival than it actually is if that person has no previous experience with the unit. Jacob, a newly-hired cyber security engineer at Unit C, a SOF headquarters element that conducts enterprise management across several service branch's special operations units, put his preconceived idea this way: "I would have thought the cyber security situation would have been locked tight, and there would be very little cyber activity directed against it," (personal communication, July 14, 2017). Elaine, a Department of Defense civilian and overall information system security manager (ISSM) at Unit N, a large naval element conducting special operations, felt similarly before beginning her work there: "I thought the unit's cyber security would be very tight" (personal communication, June 29, 2017). Most persons interviewed who had not had previous SOF experience when hired shared similar preconceptions.

2.1.2 Harsh reality

Those pre-conceived notions of the unit's cyber security competency can cause severe frustration when the new ISSM finally arrives and learns the breadth of the truth. When Elaine was hired as the first cyber security professional by Unit N to secure its information technology in 2002, Unit N had already existed for more than 15 years. The information security situation there was decidedly different from what she thought it would be. "I thought I was in IA [information assurance] hell," she said. She also described the IT environment: "NT patches were four versions behind. SNMP vulnerabilities were wide open. There was no antivirus! All our Cisco [equipment] were

past their end of life. There was no policy, no removable media control, zero security" (personal communication, June 29, 2017). For an experienced cyber security professional, such gaping lapses would be inexcusable, but for Elaine reflected the reality of the world she had joined.

Dallas, a uniformed Air Force officer and the CSIRT (Cyber Security Incident Response Team) manager at Unit C, was asked how that unit's cyber security posture compared to what he thought it would be before hiring. He simply replied, "Worse. There are too many silos to know where all the endpoints are. And, with such a disparity and spread, how do you know when you're looking at the right stuff, a true threat?" (personal communication, June 26, 2017). Once again, the disparity between pre-hire expectations and the unit's reality threatened to cause confusion and frustration.

Other SOF cyber security leaders expressed similar surprise and disillusionment. Part of the confusion stems from the SOF unit hiring process for support personnel. An interview (or skills verification, in the case of a potential contract employee) is always conducted before a hiring decision is made, but is mostly a one-sided affair. Most SOF units do not reveal all aspects of their missions or organization until the decision to hire is made and onboarding process is complete. Since the interview happens before that, unit hiring managers cannot disclose sensitive information to the interviewee, including any information that would reveal the unit's information security status or potential vulnerabilities. Although the interview usually ends with the opportunity for the candidate to ask questions of the hiring board, for legal and security reasons their answers can divulge very little about the actual nature of the information security situation. To cope, the newly-hired ISSM should strive to enter the unit with few expectations, learn the true depth of the information security situation quickly, and work to make it better once the full context is understood.

2.2 Unit culture and "the mission."

One of the most challenging aspects of integrating into a SOF unit and applying cyber security controls and procedures is understanding and blending with the unit's culture. While SOF units all differ somewhat in mission, their core functions revolve

around the United States Special Operations Command's (USSOCOM) core activities and include one or more of the following:

1. Direct action
2. Special reconnaissance
3. Countering weapons of mass destruction
4. Counterterrorism
5. Unconventional warfare (UW)
6. Foreign internal defense
7. Security force assistance
8.Hostage rescue and recovery
9. Counterinsurgency
10. Foreign humanitarian assistance
11.Military information support operations
12. Civil affairs operations (Department of Defense, 2014).

Most of these activities pose life-threatening danger to unit operators and executing them as perfectly as possible becomes the first, last, and only goal. Getting the operators “on target," at the right time, and with the right resources becomes the relentless focus of the unit, "the mission." Each SOF unit's method for delivering those operators may differ, and the manner in which the mission is accomplished will vary from unit to unit, but the mission is always paramount when describing any SOF unit. This sleepless, relentless focus on successfully accomplishing the mission creates a unique culture, even within the military. Matt, a Marine officer and commander of the penetration testing and remediation team with the responsibility to test and assist SOF units, described SOF culture this way: "Get the best people possible, give them the hardest missions the nation has to offer, resource them, and let them execute success" (personal communication, July 7, 2017). Dallas described his unit’s culture as, “Highly-motivated, intelligent people getting after complex tasks. It values independence and action, rewards boldness. The culture focuses on operational impact and being part of the mission” (personal communication, June 26, 2017). Charles, a cyber security professional with Unit C, stated that to him, the culture means, "Never a ‘no.'. When it comes to the mission, we are not in the business of saying, ‘You can't do that.' I'm not a judge. I'm an

advocate. I'll tell them a safer way to do what they want. I keep them from getting into trouble" (personal communication, June 28, 2017). Charles' attitude reflects his practical understanding that information security efforts will only succeed to the extent they are perceived by unit operators as enabling their missions, rather than hampering them.

SOF culture's single-minded "mission focus" has significant ramifications on the ability to implement cyber security. As a long-time information system security engineer (ISSE) with Unit C, when asked to describe the SOF unit culture, John's response was pragmatic: "Do it now, document it later, which turns into 'document it never,' with no regard or understanding of the risks. At subordinate units, [the] culture is crisis-action planning. It drifts into the headquarters from the subordinate units" (personal conversation, July 3, 2017). Alex, an Information System Security Manager at Unit A, an Army brigade-sized unit conducting special operations, highlighted a similar concern resulting from the "mission first" culture at his unit:

> The culture is two-fold. On a macro level, it is two classes of people – operational and support. And, at a lower level, it is squadron [subordinate unit] specific. It would seem command [highest-level unit leadership] wants there to be a unified culture of excellence, and those expectations are shared, but set at the squadron level. The contradiction also exists at that macro level in which support staff [is] treated or perceived to be of lesser standing than the operational personnel (personal conversation, June 30, 2017).

The possible perception of cyber professionals' "lesser standing" is made even more difficult by the nature of the demands of information security. When asked to describe that culture's effect on how Unit A's personnel view cyber security efforts, Alex added, "Cyber security, a position that inherently asks end users and engineers to slow production, is looked at as an impediment to operations. Anything impeding operations is looked down upon" (personal communication, June 30, 2017). Taken together, the view that cyber security support personnel are of less worth to mission success, and that information security requirements are impediments to operations, can present a daunting challenge to cyber security managers who need unit members' cooperation in cyber security efforts.

With time and effort, unit members' perceptions of information security efforts as roadblocks to operations can be overcome. Education, specifically educating unit members how unsafe actions can adversely affect the all-important mission, begins to change the perception of why cyber security professionals ask that additional steps be taken to enhance information security. Elaine said that to begin to change Unit N's view of cyber security, "I taught them how their network actions affect the mission and operations (for example, downloading games, movies, etc.) This changed the culture" (personal communication, June 29, 2017). Unit A's primary ISSM Robert related:

> All new unit members must come to the cyber security section, and I brief them on cyber efforts and risks. I put out a newsletter for the unit members' families, to help them lower their online risk profiles. I take the new personnel to the SOC [Security Operations Center] and show them how we're actually being targeted [actively scanned] (personal communication, July 5, 2017).

These examples show that with considerable effort and time, it is possible to change the cultural perception of cyber requirements to the positive. This begins with accurately depicting how good information security practices enable the unit to keep operating at its peak potential, and how poor ones put the mission at risk.

Before a cyber security professional can describe a deleterious cyber-action's adverse effect on the mission, he or she must fully understand the mission. Elaine explained:

> You must understand the mission, the requirements, and the leadership. If you come in with a checklist, you will fail. Customize it to your unit. You must know your team: their mission, what they want. You must explain what the risks are and find out if they want to accept them. For example, for team members deployed to remote locations, you may not be able to update anti-virus definitions, and you may *not* want to update mobile devices because we've seen fake updates show up in some downrange locations. This approach is contrary to DoD update policy in terms of delaying the update of a government computer, but it's operationally required (personal communication, Jun 29, 2017).

John described how fully understanding the mission could pay off by using the operators' language to educate them about cyber risks: "Teach them it's not about getting

to ‘no,' but how do we get to ‘yes.' Communicate the risks in terms they can understand, like going onto the target with side plates [bulletproof body armor] versus without side plates." (personal communication, July 3, 2017). For the cyber security professional who is new to the military or special operations, investing time early in truly understanding the mission and the unit’s language pays great dividends later in effectively communicating cyber risks and the reasons behind best practices.

Sherry is the ISSM at Unit T, a small Air Force element that conducts special operations and acts as the liaison to conventional Air Force units that periodically support SOF forces. Sherry makes a point of dealing with users at the lowest level possible, to ensure everyone in the unit knows and employs proper cyber security practices. She described her efforts to change her unit’s perception as:

> …education and training. I’ve worked to educate the end users both in my unit, and at affiliated units. I now do unannounced interviews of the users, with no retribution [if a violation is found], and ask, ‘How are you using the network? Walk me through your day-to-day processes.’ I routinely find violations or risky behavior that way. If I had just gone to ask that unit’s leadership [about their cyber security posture], they’d have just said that all was well…My role is to say these things aren't obstacles, but safeguards, and to explain how these controls make them safer. The effort in improving communication has encouraged a culture of self-reporting. They'll say, ‘Hey Sherry, check out this weird email.’ They know not to shut down the system. They even call me about suspicious items in their home networks. Again, all because we've built trust (personal communication, June 29, 2017).

These accounts demonstrate it is possible for a dedicated cyber security manager to change unit culture and perception of information security from impediment to enabler.

3. Setting the Stage for Long-Term Success

Adam Baker, abakersans@gmail.com

3.1 Build Relationships

Social skills are key in almost every profession. However, the SOF unit cyber security officers consistently referred to how surprised they were that their ability to perform their duties depended so much upon their capacity to build solid interpersonal relationships with people inside and outside the unit. Dallas remarked, "Cyber security is not a tech field, it's a people field with a technical component. Relationships are just as important as any technical control you have" (private conversation, June 26, 2017). Alex put it this way: "It's as if IT security is just a thin veneer over a much larger relationship challenge. If a relationship hasn't been built solidly, as soon as the information system goes south, the relationship sours and the problem gets worse" (personal communication, June 30, 2017). Thus, without these relationships, security efforts may be ineffective. Building interpersonal relationships can be a challenge in any high-tempo environment staffed largely with type-A personalities, and breaking in as "the new guy" is never easy. This difficulty is amplified in a SOF unit, a very tight-knit community where many experienced operators have been with their teams for a decade or more. It becomes even more challenging for the information security professional because ultimately that person will ask unit members to change how they use the network, or to do more than they are currently doing, to keep IT operations secure.

As referenced in section 2.2, making the effort to understand the unit's mission in detail and learning to communicate in the operators' language can go a long way toward creating common ground upon which a relationship can be built. Providing positive, motivating reasons for operators to comply with cyber security protocols is also key. Negative motivation, i.e., threatening an operator with a potential IA audit, is not an effective strategy for someone who routinely risks his or her life to execute the nation's most dangerous missions. Elaine from Unit N describes her successful approach: "You've got to win hearts and minds. You have to win them over. That takes a certain amount of charm, to find what's important to them. You have to social-engineer cyber security. These people don't respond to threats" (personal communication, June 29, 2017).

Unfortunately, while other entities have also cited the essential nature of interpersonal skills in conducting cyber security operations successfully, few stress the

need to pursue them in the hiring process. Indeed, the DoD's own "Cyber Workforce Strategy" document (Carter, 2013) completely excludes interpersonal skills from the list of desirable skills in a cyber security officer. Information security managers should make the ability to build relationships a key issue in hiring other cyber professionals.

3.2 "Confidence comes through competence."

Ultimately, in an environment where the unofficial motto is, "Performance is the only discriminator," all are expected to do their jobs expertly or to be tirelessly working toward that goal. Competently handling issues with a minimum of hand-wringing buys credibility as nothing else can. For example, Sherry was brought into her cyber security position at Unit T specifically because of a crisis: "Buckshot Yankee." Buckshot Yankee was the operational name given to the massive cleanup effort after a foreign intelligence service successfully planted a virus on a removable device, which ultimately infected several large US government networks (Lynn, 2010). "I was brought into the unit because of it," Sherry explained. "Somebody bought an unapproved, inexpensive (and infected) thumb drive in a foreign country, brought it back and plugged it into the classified network, and before you know it, tens of thousands of endpoints were infected" (personal communication, June 29, 2017). Sherry worked for many months of 2008 and 2009, cleaning over 3,000 systems in diverse locations. That tireless and ultimately successful effort garnered her a solid reputation in her SOF unit and gave her much more freedom of maneuver within it.

Elaine experienced a similar challenge shortly after she was hired at Unit N. Having met resistance from a senior site-lead network engineer at the unit who remarked Elaine would "just break things," she was initially denied the access required to secure a critical network. Two weeks later, that network was the only one to become infected with the Blaster virus. She was subsequently granted access and remediated the infection. After successfully doing so, she was further given the funds (and clout) to purchase and install the hardware and software necessary to secure *all* the Unit N's networks because "the Blaster infection on our network convinced leadership that cyber security was a problem" (personal communication, June 29, 2017). As Matt opined, "Confidence comes through competence" (personal communication, July 7, 2017).

Adam Baker, abakersans@gmail.com

These and other challenges allow competent cyber security professionals to show their mettle and demonstrate their value to the unit and the mission.

4. Out-smarting Manning Challenges

It should come as no surprise that as a profession, cyber security is experiencing an "unprecedented" workforce shortage (Morgan, 2017). As such, few organizations have a full quiver of cyber security talent. However, due to the incredibly high bar just to enter into a SOF unit in any capacity (e.g., the previously-referenced physical and psychological tests for uniformed and some DoD civilian personnel), SOF unit cyber security managers have great difficulty filling open positions. Even before that, not all unit leadership recognize the heavy demands placed on the few cyber security professionals they have and the danger that can arise from oversaturating a single professional. Matt, the SOF pen-test unit commander, sees the same problem in every unit he evaluates. "Lack of manning. No unit has properly manned and equipped teams. They have good tools, but you can only automate so much, and one guy can only watch so many tools" (personal communication, July 7, 2017).

Elaine illustrated the burden that the overall lack of cyber security manning places on her in her position at Unit N:

> A significant challenge is the sheer number of duties I have. I am responsible for this unit's: cyber security, CND (Computer Network Defense), cyber security workforce management (via Navy-specific personnel management requirements), Privileged User Agreement management and user training, PKI management, electronic records management [managing the documentation for all 400 of the unit personnel who fall under DoD regulation 8570], PII [Personally Identifiable Information] and FOIA [Freedom of Information Act] audits, configuration management, incident handling, the IT COOP [Information Technology Continuity of Operations Plan], forensics, and ETP [Exceptions to Policy] management (personal communication, June 29, 2017).

Such a daunting breadth and depth of duties places significant strain on a SOF cyber manager and can lead to a feeling of not performing well in any one area. As such,

manning challenges should be mitigated as much as possible through automation and federation.

4.1 Automate early and often

While it cannot completely mitigate the challenge of personnel shortages in key cyber positions, automating common tasks can at least help relieve some of the burden. Robert is tasked with securing the majority of Unit A's thousands of nodes, across multiple networks and in many austere locations, with three people. He credited his centralized automation approach for his ability to stay on top of it all. "Our structure is excellent. Our cyber controls are centralized, not scattered. I run it all (scans, etc.) Being a worldwide organization makes it difficult. Thankfully, money is not an issue. We have the dollars to buy the gear we need. However, we have multiple networks to secure and three dudes to do it with, who are IA guys, not actual CND [Computer Network Defense] guys. They're tech-savvy, but they can only do so much" (personal communication, July 5, 2017). Robert, and others, have found automation a critical component in managing cyber security efforts while working with fewer cyber professionals than they truly need.

4.2 Federate yourself

Empowering others to perform basic cyber security tasks on your behalf ("federation") can also relieve some stress on an overworked and undermanned ISSM. Sherry faces this challenge at Unit T, and finds this approach to be critical to her success. While Unit T is much smaller than Units A or N (<100 users vs. 1000+ users each), Sherry is also responsible for the SOF-specific network access requests and management for all conventional Air Force units that support SOF operations. This gives her an overwhelming number of Air Force units and personnel with whom she must engage. To compensate, Sherry designates a key tech-savvy individual as her point of contact at each unit, even if that person has no formal cyber security experience, and trains them in the basics of making cyber access requests and other necessary functions. Not only has this

partially alleviated her great burden, but Sherry's approach has also aided the enterprise managers who ultimately approve such requests. She explains, "I identify the key players at these units and develop a relationship, then educate the enterprise communications and cyber people [as to] who these units are, and what a particular element that's making a request, does" (personal communication, June 29, 2017).

> Elaine highlighted a combined example of both federation and automation: We really do have a 100% uptime requirement, on some systems, when it is needed. We've had to build in a lot of redundancy. Availability equals capability. We simply cannot have down time. This requires more preparation in terms of testing, time, etc. We've begun to automate more. [When purchasing new cyber security capabilities] we pay for professional installation on-site and training on new capabilities we purchase. We do this because we've seen folks try to save money and do it themselves (implement and learn the new system), but that learning curve impacts true availability and reliability. Our RM office [Requirements Management, the budget allocation office] understands this, and I build all of that into the cost of the buy (personal communication, Jun 29, 2017).

As much as possible, Elaine federates the task of installing and configuring new solutions and incorporates the associated extra costs and professional training in her initial budget request. This approach frees her and her staff from the time it would take to install, configure, and learn "on the job" to utilize new systems, and minimizes the impact to Unit N's daily operations. In SOF environments, personnel is the rarest and most precious asset, and any process, system or technology that keeps unit members focused on their core tasks is a force multiplier.

"Federating yourself" also means teaching the principles of secure system design to the unit's software and system engineers. If security considerations are incorporated early in the development cycle, there are less likely to be large vulnerabilities the new equipment and software which must be mitigated (much less efficiently) just before launch. This approach also requires less remediation effort from the cyber security professional. John, a senior ISSE at Unit C, said, "If I can grow an ISSE mindset [in the developers], incorporating cyber security in project engineering and design phase, from kickoff, that will help a lot" (personal communication, July 3, 2017). John and others

have found that investing early in secure design pays great dividends in saving time and effort down the road.

4.3 Recruit from within the unit…and be ready to train

With such significant barriers to entry into the SOF world, in addition to traditional talent search methods, information system security managers in SOF units should look to fill their open positions from the pool of those who are "inside the wire," people who are already members of the special operations community. The cyber security workforce shortage has made information security one of the most in-demand fields in IT, and as such may be attractive to tech-savvy uniformed, civilian, and contract employees working in other capacities at the unit. Several current SOF unit cyber professionals came into their current positions from other, non-cyber specialties. However, a wise cyber security manager will formulate and systematize the continuous internal search for the next new hire.

Once such a person is laterally-hired from within the unit, they will obviously need training before they can adequately fill a cyber security position. Part of the systematic recruiting approach should be a formalized training plan, customized by position. The GIAC Certification Roadmaps (GIAC, 2017) are an excellent resource for domain-focused cyber security training plans.

5. Know the Regulations, and How to Bend Them (Legally)

SOF units keep standard human resources data for their members, such as those that are subject to HIPAA and Personally Identifiable Information (PII)-related regulations, but that's just the tip of the iceberg. SOF units' information system operations are also subject to DoD cyber security regulations 8500, 8140, 8570.01-M, ICD503, service-specific requirements (Army, Navy, etc.) and any regulations or Standard Operating Procedures (SOPs) issued by the headquarters element. Beyond all of these, SOF unit cyber security professionals must also navigate the various stakeholder organizations' interpretations of those regulations. John captured it this way, when asked what he

wished he'd known before taking a cyber security position at his SOF unit: "I wish I'd had a better understanding of how different people in the enterprise viewed RMF [Risk Management Framework]...everyone interprets the special publications differently (the local view, vs. the DIA [Defense Intelligence Agency] view, vs. the SOCOM view, etc.)" (personal communication, July 3, 2017). While it is a daunting task, a SOF cyber security professional must read and understand each of these regulations and policies, and further work to understand how each entity expects them to be followed.

Because of SOF's unique missions, and disparate and austere working environments, exceptions will have to be made in complying with some regulations. In order to pursue those exceptions legally, they must first be known and fully understood; the mechanisms for employing an exception must be utilized and documented. For example, for a time after Buckshot Yankee, the DoD completely prohibited the use of removable media in government information systems. Unfortunately for some SOF air units, removable media was the only way to transfer data to and from some aircraft systems. The DoD subsequently allowed an "Exception to Policy" (ETP) to the removable media ban, under strict guidelines (Alexander, 2013). Using this mechanism allows the unit to proceed with the mission while operating within the law.

Another example is the DoD policies requiring information systems receive patch updates as soon as the patch is available. While this is possible for conventional units in the continental United States (CONUS) who have consistent internet and network connectivity, it is a pipe dream for a SOF unit with multiple nodes deployed in austere overseas environments, with limited or infrequent network access. While some in the oversight chain might cringe at having a significant number of unit systems unpatched and in the field, such flexibility based upon mission requirements is part and parcel of SOF unit cyber security operations. To lose that flexibility would be to risk losing that SOF unit's ability to rapidly respond to an emergent situation in a distant location, or to quickly shift assets to a new theater of operations. Robert remarked, "Higher headquarters staff try to tell me how to run my stuff, who don't understand what my unit's operators are doing and where they are. My numbers aren't going to be perfect. I'm ok with that. I'm afraid the enterprise is losing its agility and becoming 'conventional'" (private communication, July 5, 2017). Robert can comfortably take that position because

of his knowledge of the appropriate regulations and policies, and his unit commander's attitude toward cyber security risk versus mission accomplishment. Each SOF unit's ISSM must understand the same for their unit.

6. "Welcome to a Higher Risk Tolerance"

Nearly all SOF unit cyber security managers stressed the importance of building a relationship with their unit's leadership. Ultimately, the only reason any person in the unit has authority to do their job is because it has been delegated by the unit commander. The SOF unit's ISSM will act to secure the network and mitigate risk, but ultimately, if the commander decides that the mission trumps cyber security in some aspect, that is his or her decision to make. This is why the ISSM must have a good working relationship with the commander, the deputy and assistant commanders, and possibly a chief of staff. The commander will determine the overall risk tolerance level for the unit, and the ISSM will implement strategies congruent with that risk tolerance.

The ISSM must also transparently communicate what kinds of risk, and how much of it, a potential course of action will engender. Making these clear permits the commander to make an informed decision. It can also protect the ISSM from any accusations that the commander was not fully informed of the risks, in the event of a security violation or incident.

Since most SOF units value initiative, once the commander's risk tolerance level has been communicated, the ISSM normally has a near-complete freedom to implement solutions that secure the environment, in accordance with the commander's intent. That freedom is something that motivates SOF unit ISSMs to strive for excellence and is one of the aspects of the job they enjoy most. Robert, ISSM for Unit A, sums it up: "Welcome to a higher risk tolerance. I can get away with a lot more than anyone else I know. I'm empowered to make decisions most people can't, vice big DoD regulations that would hamper our operations" (private communication, July 5, 2017).

A solid relationship with the commander is also an important enabling function for pursuing needed cyber security initiatives. As John puts it, "Never underestimate

senior leader proponency and advocacy for your effort, regardless of what it is. If your own leader isn't an advocate for what you're doing, you're not likely to get [the] necessary support from other directorates. Senior leaders may tell you, "That's a great idea, but not for right now" (personal communication, July 3, 2017).

The leader's attitude will come to define how seriously the unit members view cyber security. Julie, the A&A (Authorization and Accreditation) officer for Unit C, remarked how her unit's attitude had shifted based upon senior leader emphasis: "It was trending positively when a GO/FO [General Officer/Flag Officer, for example, an Admiral] was interested and preaching it. After he left, the [cyber security] effort left with him" (personal communication, July 5, 2017). Because so much depends upon how highly senior leaders prioritize information security, a savvy cyber security professional will seek out those who express interest in cyber efforts to foster a trust relationship and pursue advocacy for needed initiatives. Paradoxically, when dealing with senior leaders who does not place as high priority on information security efforts, cyber security incidents (and their fallout) can motivate senior leaders to take a greater interest and become more active in mitigation efforts. Cyber security managers should look for every opportunity to educate and influence their senior leadership toward securing the operating environment.

7. Always Be Marketing

Another important aspect of the overall cyber security programs implemented by SOF unit ISSMs is a comprehensive marketing or public relations plan. Matt, the officer whose pen-testing and remediation team must demonstrate its competence and value across every SOF unit they evaluate and remove the naturally-threatening perception of being "the people that will see the unit network's vulnerabilities", met with unit cyber representatives at every opportunity. Members of his unit presented at SOF-specific cyber conferences and took an active role in the wider Cyber Security Work Force meetings and training. He ensured all his team members' communications with SOF units were positive. "I tell my guys we're all sunshine, rainbows and unicorn farts. [Our

unified message is], ‘we don't care how messed up you are when I get there, we care how messed up you are when we leave.’"

Based on comments from SOF ISSMs, a comprehensive intra-unit cyber security marketing plan might include:

1. A weekly or monthly email newsletter to unit members highlighting cyber security incidents, successes, and calling out news stories of cyber events
2. Initial training for new unit members that shows active threats
3. Regular newsletters and/or classes for unit members’ families that focus on ways to reduce their risks online, and teaches resistance to social engineering techniques
4. Custom training, in addition to DoD-mandated cyber security awareness training, that shows unit-specific examples of past cyber threat activity and mitigation (private communications, multiple dates)

A final critical piece of the cyber security marketing strategy is to regularly look for specific instances where unit purchases of cyber security systems were successful in mitigating a threat, and sincerely thanking the unit leadership and acquisition personnel for them. Not only is this a great social skill in practice, but saying, “Thank you for allowing us to make this purchase; this is how it just thwarted an attack against us” serves several purposes. Including the unit’s acquisition team in the expression of gratitude dispels the feeling that the ISSM only ever asks for more (and more expensive) equipment, by giving a visible example of how an item already purchased was used to further the unit’s mission. For the leadership, it reinforces confidence in the wisdom of the ISSM’s recommendations in the first place, and “greases the skids” for further purchase approvals when necessary.

8. Conclusion

Taken as a whole, the common strategies employed by SOF ISSMs provide a comprehensive guide to avoiding the major pitfalls, and bring a higher probability of

success to cyber security professionals in a special operations environment. The distilled lessons that form the "road map" to success are as follows:

1. Realize going in that the cyber security effort at the unit may not be nearly as mature as the core areas of the mission.
2. Build solid relationships with unit operators and key players as early as possible. Begin with interpersonal skills, and understand that in a SOF unit, nothing accomplishes this quite like being competent.
3. Work to completely understand the unit's mission and culture before imposing major changes, barring a major cyber security incident.
4. Pursue every opportunity to federate and automate as many duties as possible.
5. Actively seek out tech-savvy unit members for recruitment into the cyber security field. Create a training plan for each member of the team that focuses on creating competency and ultimately attaining (and maintaining) mastery.
6. Know all the regulations that apply to your unit, cold. Apply them to the maximum of their legal flexibility to accomplish the mission.
7. Develop a good working relationship with, and seek every opportunity to educate, the commander and his senior leaders. Honestly and transparently communicate risk levels of various courses of action under consideration. Respect the commander's ultimate decision.
8. Create and employ a comprehensive marketing plan for your cyber security efforts.

While securing the information systems and activities of a special operations unit may be one of the most daunting tasks in the cyber security profession, it can also be one of the most rewarding. There is little that compares to enabling the nation's finest warriors to safely and successfully execute their missions, again and again. SOF units expect their cyber security professionals to be proactive, flexible, professionally curious, intellectually aggressive and technically superior. It isn't for everyone. But maybe, if you're one of the best, it's for you.

Adam Baker, abakersans@gmail.com

References

Alexander, David (2013). Reuters.com, "Pentagon Flash Drive Ban has Many Exceptions." Retrieved on Aug 17, 2017, from http://www.reuters.com/article/us-usa-security-pentagon-idUSBRE95L06520130622

Basani, Vijay (2016). EiQ Networks Blog, "Here Are the Skills You Need to Be a Chief Information Security Officer." Retrieved on Aug 17, 2017, from https://blog.eiqnetworks.com/blog/here-are-the-skills-you-need-to-be-a-chief-information-security-officer.

Department of Defense (2013). *DoD Cyber Workforce Strategy*. Retrieved on Aug 17, 2017, from http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed%28final%29.pdf

Department of Defense (2014). *Special Operations*. Joint Publication 3-05. Retrieved Aug 17, 2017, from http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf

Department of the Army (2013). "Female Volunteers for the United States Army Special Operations Command (USASOC) Cultural Support Teams (CST)." Retrieved Aug 18, 2017, from *www.soc.mil/CST/ALARACT%20258.doc.*

Fuentes, Gidget (2015). San Diego Union-Tribune.com, "The Army's Secret Weapon: Special Forces." Retrieved Aug 17, 2017, from www.sandiegouniontribune.com/military/sdut-armys-secret-weapon-special -forces-group-2015aug04-story.html

GIAC. *Get Certified: Roadmap*. Retrieved Aug 17, 2017, from https://www.giac.org/certifications/get-certified/roadmap

Lynn, William J. III (2010). Foreign Affairs.com, "Defending a New Domain." Retrieved Aug 17, 2017, from https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

Adam Baker, abakersans@gmail.com

Morgan, Steve (2017). CSOOnline.com, "Cybersecurity job market to suffer severe workforce shortage." Retrieved Aug 17, 2017, from http://www.csoonline.com/article/3201974/it-careers/cybersecurity-job-market-statistics.html

Trevithick, Joseph (2014). "The US Army has Quietly Created a New Commando Division-1st Special Forces Command brings together thousands of Green Berets." Retrieved Aug 17, 2017, from www.medium.com/war-is-boring/the-u-s-army-has-quietly-created-a-new-commando-division-2b90961b4821.

Adam Baker, abakersans@gmail.com

Appendix A:
Interview Schedule

Interviews were conducted with the following individuals on the dates specified below, via phone, email, or face-to-face communications:

Dallas, Unit C, June 26, 2017

Charles, Unit C, June 28, 2017

Sherry, Unit T, June 29, 2017

Elaine, Unit N, June 29, 2017

Alex, Unit A, June 30, 2017

John, Unit C, July 3, 2017

Robert, Unit A, July 5, 2017

Julie, Unit C, July 5, 2016

Matt, penetration test/remediation unit, July 7, 2017

Earl, Unit L, July 12, 2017

Jacob, Unit C, July 13, 2017

George, Unit C, July 14, 2017

Adam Baker, abakersans@gmail.com

Appendix B: Interview Questionnaire

1. Name
2. Unit description
3. Unit size (approx.)
4. Education Level
5. Certifications
6. Years in cyber security
7. What brought you into cyber security?
8. Position before coming to the unit (or before taking a cyber security position at the unit):
9. How long at the unit?
10. Why were you hired (a new position, to replace someone, or because of an emergency?)

Initial Unit State of Cyber Security Upon Hiring (e.g., personnel perception of cyber security, etc.)

1. Before you came on board, what did you think the cyber security situation would be at the unit?
2. Approximately how many cyber security personnel worked at the unit?
3. Once hired, was the reality different from what you expected? If so, how?
4. What was your first "crisis" in cyber security at the unit?
5. How was it resolved?

Adam Baker, abakersans@gmail.com

6. How did it affect your perception of the unit, or of cyber security at the unit? If so, how?

Unit Culture's Effect on Cyber Security

1. How would you describe the overall culture of your unit?
2. How does that culture affect how unit personnel views cyber security **efforts**?
3. How does that culture affect how unit personnel views cyber security **personnel**?
4. Has the unit's perception of cyber security changed over time? If so, how, and why?
5. How does unit culture affect your efforts to increase cyber security?
6. What efforts have you made to change your unit's perception of cyber security efforts and requirements?
7. How have your efforts been received?
8. If you could change one thing about your unit's overall culture (in regards to how it affects cyber security), what would it be?
9. What plans do you have, moving forward, to change unit culture or perception of cyber security (if any)?

Unit Design

1. How does the organization of the unit help/hinder cyber security?
2. If you could redesign one thing about the unit to improve cyber security, what would it be?

Adam Baker, abakersans@gmail.com

Unit Cyber Security Posture, As Viewed Through CIS Controls

1. Inventory of Authorized and Unauthorized Devices	11. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
2. Inventory of Authorized and Unauthorized Software	12. Boundary Defense
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	13. Data Protection
4. Continuous Vulnerability Assessment and Remediation	14. Controlled Access Based on the Need to Know
5. Controlled Use of Administrative Privileges	15. Wireless Access Control
6. Maintenance, Monitoring, and Analysis of Audit Logs	16. Account Monitoring and Control
7. Email and Web Browser Protections	17. Security Skills Assessment and Appropriate Training to Fill Gaps
8. Malware Defenses	18. Application Software Security
9. Limitation and Control of Network Ports, Protocols, and Services	19. Incident Response and Management
10. Data Recovery Capability	20. Penetration Tests and Red Team Exercises

1. Looking at the CIS controls above, what was the overall state of unit cyber posture when you arrived?

2. What 2 or 3 (or more) controls do you view **were** the most critically-lacking when you joined the unit?

3. Why do you think they were deficient?

4. What did you do to address them?

5. How does the unit cyber security today compare to what it was when you were hired?

Adam Baker, abakersans@gmail.com

Special challenges

1. Describe any challenges you see as unique to your unit or position

2. Describe how you have addressed them

Conclusion

1. How does the unit's overall cyber security now (culture, technical controls, training, etc.) compare to what it was when you were hired?

2. Is there anything we have not covered in this interview that you think has helped change the cyber security posture for the better?

3. What do you wish you had known when you were hired about improving cyber security in the unit?

4. Is there anything else we haven't addressed, that you think cyber security professionals who are new to this kind of unit should know?

Adam Baker, abakersans@gmail.com

Last Updated: November 19th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS London November 2017	OnlineGB	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced