What Makes a Good Security Leader?

Introduction

The list of traits attributed to great leaders is long and varied indeed: courage, strength, intelligence, honour, energy, adaptability, innovation, initiative – and there are many, many more. In fact, when it comes to discussing leadership attributes, journalists, historians and social scientists seeking to chronicle and analyze the exploits of great leaders are constrained only by vocabulary and imagination. To attempt to define any single set of leadership characteristics is to risk oversimplification. Certainly, situational factors such as available resources, environment, team capabilities, and more often than not, the less tangible factor of luck – being at the right place at the right time - all combine to make a successful leader. However, there are certain predominant characteristics that we have found common in successful ***security*** leaders. This article will examine a few of the key leadership principles for the security professional, and explain why choosing your security leader wisely is critical to your organization's success and, quite possibly, its survival.

Leadership Defined

Leadership means many different things to many different people. There are just as many leadership definitions as there are people and organizations claiming to understand and practice this social phenomenon. Given our military background, we at Presidia tend to view leadership as "the art of influencing people to act in accordance with one's intent for a shared purpose."[1] In essence, leadership boils down to the ability to inspire others to achieve a common goal. You don't have to be in the military to see examples of strong and inspirational leaders – they are all around us, in industry, in government, in not-for-profit organizations, in our social circles, and in our educational and research institutions.

Leaders are the ones we look to for inspiration, guidance, reassurance and hope in the face of adversity. They see opportunity and exploit it. They build teams and unify people to achieve common goals, and they mentor others to ensure a bright future. They are the trailblazers, the innovators and the rally points for realizing potential and making the world a better place.

[1] Canadian Forces Leadership Institute, *Leadership in the Canadian Forces - Doctrine*, © Her Majesty the Queen in Right of Canada, 2005, p. 3.

Essential Traits for Security Leaders

One might argue that "a leader is a leader" – that leadership attributes are universal and that all leaders display similar traits regardless of their vocation or profession. This may very well be true. However, in our experience examining numerous government, corporate, not-for-profit, and policing and security agencies, Presidia's principals have found common, predominant traits in the many successful security leaders we have met over the years. What follows are what we believe to be some of the key attributes that you should be looking for in your organization's security leader.

Knowledge and Skills

The successful security leader is knowledgeable about threats and risks to the people, information, assets and reputation of their organization, and has the skills to quickly identify vulnerabilities and employ effective and efficient countermeasures. They will have an intimate understanding of the organizational objectives and how they are achieved. They will also have the ability to look at the security program holistically, carefully balancing the organization's goals with acceptable residual risk. The successful security leader will be networked and acutely aware of current industry trends, with the appropriate education, training and experience to be able to quickly adapt to the dynamic threat environment. While it is rare to find an individual who has in depth knowledge across all the security disciplines or sub-specialties (personnel security, physical security, Information/information technology and cyber security, transportation security, material/logistics security, and security program management), a good security leader will seek out and engage expertise in each of those areas. The security leader must demonstrate unwavering attention to detail, for the consequence of error is great.

Intelligence and Vision

The successful security leader must be smart – and be able to think on his or her feet. They must have finely-honed cognitive and analytical skills to be able to quickly grasp abstract concepts and develop innovative solutions to thorny or unusual problems. Creativity and imagination are traits that fall under the category of intelligence, as the security leader must carefully develop contingency plans and assess potential threats and risks to the organization's operations. Situational awareness and adaptability are also key to ensuring the ongoing protection of the organization's people, information, assets and reputation.

The difference between a successful security *practitioner* and a successful security *leader* is significant: it is the difference between a gifted musician and a gifted orchestra conductor. While usually also a talented musician, the conductor, through careful arrangement and synchronization, brings all the orchestra's instruments together to create a symphony. In an

organizational context, the security leader is the conductor. He or she must be able to process vast amounts of information, plan the overall security "campaign", and synchronize the actions of the many different security elements at decisive points to achieve operational and strategic security objectives.

Moral Courage

Security leaders hold the proverbial "keys to the kingdom" in that they are entrusted with protecting an organization's most precious assets: people, information, facilities, operations and reputation. They will also likely be responsible for compliance programs and/or enforcement of policies, regulations or other legislative requirements. This requires moral courage: the ability to make ethical decisions and always do the right thing, no matter how hard or how unpopular. The security leader tells the executive authorities what they *need* to hear, not what they *want* to hear; this has been a tenet of security leadership long before the whole "Speak Truth to Power" movement. The security leader is often a moral compass for an organization because the security profession must engender trustworthiness, honesty, integrity and professionalism to be effective.

Honesty and Integrity

Honesty and integrity are at the very core of the security profession—and they must always be the foundation upon which the security leader and his or her organization functions. Integrity and honesty lead to trust, which allows the security leader to effectively perform his or her duties, ensuring that security can enable an organization's operations. The security leader will guard his or her integrity with all their might because, like trust, once it is lost, it is lost for good. Integrity and honesty must be apparent in every aspect of the security leader's life – both on and off duty. This is also known as "Leading by Example."

Interpersonal Skills

The successful security leader must have finely-honed interpersonal skills. He or she must be a "people person" – approachable and sociable, and ensuring that their genuine concern for the well-being of others comes through. His or her communications skills must be exceptional to be able to articulate risk management strategies to executives and tactical security team goals to subordinates. Moreover, he or she must be an excellent listener and observer, picking up on subtle verbal and non-verbal cues. A large part of the security leader's mission is dealing with sensitive personnel issues. He or she must always remember that there is a person, a life, and a family behind every file number. For this reason, the security leader will act with the utmost of discretion, compassion, and will treat people with respect an dignity at all times. The individual entrusted with these responsibilities must be able to inspire trust and confidence. They must be confident, firm, fair and friendly – and have a good sense of humour.

Institutional Acumen

In order to achieve the true security mission – which is supporting the overall organization's success, the security leader must be a visionary, entrepreneur and have an intimate understanding of organization's mission, vision and values. He or she must also comprehend the roles, responsibilities and authorities of the executive cadre. This includes being attuned to the personalities and political nuances that are found in all organizations. He or she must have unfettered access to key leaders in order to effectively communicate potential threats and risks to the organization; however, the successful security leader will be able to distinguish between executive-level concerns and day-to-day, routine operations. The security leader will quickly establish a personal rapport with those key influencers within the organization – with a view to supporting mission success. The security leader will anticipate future security trends with imagination and realism, and will establish a strategic direction for the security program. He or she will set achievable goals, effectively matching the resources assigned to the security program in order to construct a viable, intelligence-led security program – one where security strategies are based upon the acquisition of intelligence (threats, risks, and vulnerabilities) through engagement with the organization's personnel, by networking with supporting agencies, and by taking a proactive approach to security awareness and training.

Conclusion

Leaders are individuals who are able to inspire others to work together to achieve common goals. Whether leading a small team or a large, complex organization, the value of good leadership cannot be overstated. This holds true for security organizations, as well. Good security leaders will not only positively influence their security team members to diligently protect their organization's people, information and assets, they will positively influence their organization – and their organization's leaders – to appreciate and understand the important role that security plays in mission success. A good security leader will display many leadership traits. Among the most important are: knowledge and skills; intelligence and vision; moral courage; interpersonal skills; honesty and integrity; and, institutional acumen. These are qualities that you want in your security leader.

About the Author

James LEGERE

James is a policing and security specialist with more than thirty years of experience. He has conducted police and security operations both domestically and internationally. His broad international experience includes tours in the Golan Heights, Geilenkirchen, Germany and two tours with the American military.

Additional Articles from Presidia Security[2]

Ask The Question – What is My Security Strategy?

Security is often thought of as a tactical issue that should remain at the "gates and guards" level. While these tactical security pieces may be important they are most effective as part of a security strategy that is designed to mitigate the threats and risks to your company and its operations. True security strategy is integrated into a company's "C Suite" and is seen as an enabler. The questions and discussion that follow outline the framework for a company security strategy.

Assessing and Tracking Threats - Protecting Your Employees and Your Company

Recent incidents of violence in the workplace in Canada tragically illustrate what happens when threats materialize into actions; they serve as a stark reminder to businesses across the country of their responsibility to protect their employees in the spirit of "due diligence" and "due care and attention." Rarely, if ever, do these violent situations manifest themselves without some sort of prior indicators. This underscores the importance of having proper procedures in place to track and assess threats to your employees. Take the time to review the following recommendations to determine whether your company is prepared to address threats to employees.

Executive Protection Considerations

In today's fiscally challenged business environment it may be difficult to justify providing an Executive Protection Program for an organization's key executives. However, in making this important decision one also has to consider what the cost would be to the organization's bottom line and, perhaps more importantly, to its reputation should a key member of the senior leadership team be the target of an act aimed at harming or embarrassing the individual and the organization.

Due Diligence Investigations

If asked, many companies would say that they have "due diligence investigation" processes in place; however, these processes are often designed to review the financial and operational affairs of a particular company and fail to closely inspect the background of the main principals or executives of the company. In addition, many companies do nothing more than cursory checks on individuals they are about to hire. The lack of a robust background investigation can result in wasted time and can cause legal and financial problems. There is an abundance of legal findings across Canada, as well as internationally, that clearly articulate the liability facing companies who do not carry out appropriate due diligence investigations. In order to inspect this issue closer one must first begin with a definition and understanding of what "due diligence" consists of.

[2] Available online at our website: www.presidiasecurity.com/library.html

Take a Moment to Celebrate Success

Take a moment today to think about the successes you have had and the team that got you there. It is well worth it.

A Solid Foundation for Administrative Investigations

"Is it time for the implementation of standards, including proper training and oversight, as it pertains to the conduct of "administrative investigations"? It could be argued that administrative investigations are purely "administrative" in nature and as such there is no requirement for an enhanced capability. However, it can also just as easily be argued that these types of investigations can have a very negative impact on the lives of those being investigated, including the potential loss of their livelihood. They also bring with them a large degree of "personal and institutional liability" on the part of those individuals conducting the investigations and the" "organizations for which they are employed."

Marine Port Security - Published in FrontLine Magazine

"Since 9/11, marine port security has been the subject of increased scrutiny as it is clear that contraband flows - undetected and uninterrupted - through access and egress points of both Canada and the United States. Numerous reviews initiated by the United States Government Accountability Office (GAO) and the Canadian Standing Senate Committee on National Security and Defence have clearly articulated that ports are a haven for criminal activity and organized crime, as well as targets for potential terrorist activity. Both these reviews demand an increase in the level of intelligence sharing among partner agencies focused on policing and security of marine port operations."

Setting up an Intelligence Hub - Published in FrontLine Magazine

Intelligence in some form is in use today across a broad spectrum. No longer just the purview of Government entities, business intelligence is a common term and practice among corporations. Today, in the internet age, there is an abundance of readily accessible information about any given topic, organization or person. The immense growth of social networking in recent years has added to a rich information bank that is readily accessible to anyone with an internet connection. The challenge today is to sift through vast quantities of information to uncover and piece together the information you require into an intelligence picture that supports your operations. The value of your own information can increase exponentially when combined with open source research and information from other entities with whom you are willing to share.

Security Policy

"Policy writing: next to cleaning the coffee break area, doing personnel assessments or wrestling a hungry grizzly bear, it is probably one of the least desirable tasks in any organization. Its mere mention can send employees scrambling over desks and seeking cover in the hopes of being spared the mind---numbing drudgery of documenting the company's rules, procedures and practices. There is a good reason for this: writing is hard work – and writing clearly, concisely and meaningfully is even harder still. When it comes to communicating an effective security policy, capturing that policy on paper (or, in today's digital

environment, electronically) is only the first – albeit most critical – step. Disseminating the policy and ensuring compliance are close second and third priorities, followed by periodic reviews to ensure the aforementioned policy continues to meet your organization's requirements. "

Travel Security

"Media reports continue to include stories about company executives, oil field workers and regular travelers who have been the victims of kidnappings, armed robberies and murder while visiting foreign countries. Recent events have seen a Canadian woman kidnapped in northern Nigeria and her captors demanding $136,000 for her release. This woman was a financial advisor who was in Nigeria with other Canadians as part of an exchange program and she was kidnapped as she was entering a house after attending a social event. There are also ongoing reports of oil workers being kidnapped by rebels in South America and Africa; it would appear that these types of incidents are increasing rather becoming a thing of the past. "

Duty of Care

"The dynamic threat environment that persists in today's business climate demand constant vigilance and discipline. Under the Canadian Criminal Code, companies owe a duty of care to their employees. This means businesses must take "reasonable steps" to protect workers, whether they are in Canada or working internationally. If companies do not meet this duty of care, they can be found criminally and financially liable under the Criminal Code. In the most extreme cases, the company can face hefty fines and the executives can be prosecuted and potentially jailed. In addition to the criminal prosecution, individuals can also face personal civil litigation. "