INTRODUCTION

What is a CISO?

What is War?
• The pen may be mightier than the sword, but the budget is mightier than the pen.
• Lightening, water and people always follow the path of least resistance.
• IT is the 8th layer
• There is always another rock to turn over. Don’t make more rocks.
• If your position changes based on circumstance, then you need to rethink your position.
• No, is not forever.
I. LAYING PLANS

Sun Tzu wrote:
The art of war, then, is governed by five constant factors, to be taken into account in one's deliberations, when seeking to determine the conditions obtaining in the field.

These are: (1) The Moral Law; (2) Heaven; (3) Earth; (4) The Commander; (5) Method and discipline.

Scott Tzu says:
The art of IT Security, then, is governed by five constant factors, to be taken into account in one's deliberations, when seeking to determine the condition of your company.

These are: (1) Policy; (2) Culture; (3) The Internet; (4) The CISO; (5) Budget and organization.
II. WAGING WAR

Sun Tzu paraphrased:
*Long drawn out campaigns cost too much and are bad for morale and should be avoided.*

Scott Tzu says:
*Because this war will never end, we must redefine both victory and defeat.*
Sun Tzu wrote:

If you know the enemy and yourself, you need not fear the result of a thousand battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

Scott-Tzu can’t improve on that wisdom, but I will expand on what it means in our context.

While the CISO is important, the ‘yourself’ referred to here goes beyond personal self to your department, business unit, company & industry.
III. THE SHEATHED SWORD CONT.

Sun Tzu wrote:

*He will win who knows when to fight and when not to fight.*
*He will win who knows how to handle for superior and inferior forces*
*He will win whose army is animated by the same spirit throughout all its ranks.*
*He will win who, prepared himself, waits to take the enemy unprepared.*
*He will win who has military capacity and is not interfered with by his sovereign.*

Scott-Tzu says:

*He will win who knows the fight is never ending.*
*He will win who knows how to handle both sophisticated and unsophisticated adversaries.*
*He will win whose department is motivated at the same level throughout all its ranks.*
*He will win who, when not seeing evidence of compromise seeks that which is hidden.*
*He will win who has IT Security capacity and is not micromanaged by his boss.*
IV. TACTICS

Sun Tzu wrote:

*The good fighters of old first put themselves beyond the possibility of defeat, and then waited for an opportunity of defeat the enemy.*

Scott Tzu says:

*Failure is the inability for a CISO to know the true condition of their current state and be able to respond appropriately to compromise. Waiting, without searching for the truth of your condition is surrendering without a fight. A lesser failure is knowing the current state but lacking a strategy for improvement or having a strategy, failing to secure funding to execute.*
Sun Tzu wrote:

*The control of a large force is the same principle as the control of a few men: it is merely a question of dividing up their numbers.*

Scott Tzu says:

*Every company is different both in amount of resource and in workload. Use a risk based approach to triage compromises. Focus too much on remediation, and you never discover root cause, spend too much time on investigation and too much data is lost.*
VI. WEAK POINTS AND STRONG

Sun Tzu wrote:
*He who can modify his tactics in relation to his opponent, and thereby succeed in winning, may be called a heaven born captain.*

Scott Tzu says:
*He who knows his own environment and has deployed the proper balance of protection, detection, investigation and remediation tools and processes and can adapt to the changing tactics of their adversaries may be called a heaven born CISO.*
VII. MANEUVERING

Sun Tzu wrote:
Maneuvering with an army is advantageous; with an undisciplined multitude, most dangerous.

Scott Tzu says:
It is critical that all members of your department are skilled and that the goals and objectives are clear and understood by all. Leaders must develop their staff and keep them informed to the point that if they leave, they are easily replaced.
VIII. VARIATION IN TACTICS

Sun Tzu wrote:
When in difficult country, do not encamp. In country where roads intersect, join hands with your allies. Do not linger in dangerously isolated positions. In hemmed-in situations, you must resort to stratagem. In a desperate position, you must fight. There are roads that must be followed, towns that must not be besieged.

Scott Tzu says:
When earnings suffer, don’t request more capex and opex. Where possible, leverage existing IT vendors to fulfill product needs and try to wrap in security tools as part of a bigger deal. If you get headcount, fill it fast before a freeze or challenge hits. When pushed for justification of existing program, make sure to have the metrics and business cases already written. There are meetings that must be attended and battles that are not worth fighting.
IX. ARMY ON THE MARCH

Sun Tzu wrote:

He who exercises no forethought but makes light of his opponents is sure to be captured by them.

Scott Tzu says:

The A in APT is about the people behind the attack, not the sophistication of the malware. It is as sophisticated as it needs to be in order to work, and not one bit more.
X. TERRAIN

Sun Tzu wrote:
We may distinguish six kinds of terrain: accessible ground; entangled ground; temporizing ground; narrow passes; precipitous heights; positions at a great distance from the enemy.

Scott Tzu says:
There are six types of security posture: clueless (intentionally or unintentionally); aware but unwilling; lip service; working a roadmap; strong posture; complacent.
XI. THE NINE SITUATIONS

Sun Tzu wrote:
*The Art of War recognizes nine varieties of ground: dispersive; facile; contentious; open; intersecting highways; serious; difficult; hemmed-in; desperate.*

Scott Tzu says:
*IT Security recognizes nine vectors: application; presentation; session; transport; network; data link; physical; insider; 3rd party*
XII. ATTACK BY FIRE

Sun Tzu wrote:
*There are five ways to damage the enemy with fire: soldiers in camp; stores; baggage train; arsenal and among the enemy in battle.*

Scott Tzu says:
*The enemy can hold our data for ransom or simply destroy it out of malevolence. Unlike physical fire, a robust DR plan can protect against this type of attack.*
Sun Tzu wrote:
To remain in ignorance of the enemy’s condition, simply because one grudges the outlay of a hundred ounces of silver in honors and emoluments, is the height of inhumanity.

Scott Tzu says:
There are many free sources of threat intelligence, but while some are good, you also get what you pay for so don’t be stingy.
The Art of War is not just a guide to waging war, but a reference for self improvement and life strategies. The study of its lessons should be repeated over time, as your circumstance changes and wisdom is gained, you shall see the writings in a new light.

http://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/Appendix-F.txt
QUESTIONS?
ABOUT SCOTT TZU™

- EOD – Army (5 years)
- Interrogator/RU Linguist/PSYOP – Army Reserve (9 years)
- Security Officer – Honeywell (college years)
- Director of Security – Walker Methodist (2 years)
- Security Consultant, Security Manager, Director of Security, Director of Enterprise Security – Xcel Energy (9 years)
- CSO – ATK (5 years)
- Adjunct Instructor – St Mary’s University of Minnesota (4 years concurrent with ATK)
- VP, Head of Enterprise Security Services – Thomson Reuters (2.83 years)
- MA, CPP, CISSP
- Husband, father, writer, hunter, shooter, gamer, public speaker, brewer and a treasure trove of useless movie references and other odd facts.
- scott.mccoy@thomsonreuters.com