Secureworks®

WHITE PAPER

Applying the “Doctrine of Maneuver Warfare” to the Execution of a Cybersecurity Action Plan

Why It’s Time for a Warfare Approach to Cybersecurity

CFOs, like CEOs, care most about their organization's brand and the safety of their clients' data. That's because any damage to either one will negatively impact the top and bottom lines. The same is true for our country. We want to protect our nation's reputation and the safety of our citizens and will go to war with any adversary that threatens either.

Our digital information system is under attack by malicious interlopers who wish to inflict financial and reputational damage for their own gain. Hackers are targeting private information because of its profitability and the ease of obtaining it. With escalating phishing and malware attacks and the rapidly expanding strains of ransomware, our enemies are now turning to non-malware attacks.

In conjunction with the rise of ransomware and the continued ubiquity of mass malware, attackers are increasingly utilizing non-malware attacks in an attempt to remain undetected and persistent on organizations' enterprises.

One of the most notorious examples of a "fileless" or non-malware attack was the 2017 Equifax breach, in which a command injection vulnerability created the exploit, allowing for remote execution of code so that external hackers could manipulate an open-source enterprise software called Apache Struts. The scope of the data breach was unprecedented, and Equifax faces staggering costs from regulatory fines and legal expenses for an ongoing class-action lawsuit. The event single-handedly triggered a national conversation about regulatory improvements.

This war started while we weren't looking. If CFOs and CEOs want to protect their brand and the confidence of their customers, they need to adopt a military mindset. In a recent article by Secureworks and Clearwater Compliance entitled "Justifying Cybersecurity Investment with a Warfare Mindset," we presented a protection strategy and framework based on a war mentality, along with a methodology for calculating the return on an investment in cybersecurity.

Our cybersecurity experts have outlined specific operational tactics that can be applied to this framework, along with the benefits of these risk mitigation activities.

The successful information security leader is able, through preparation resulting from "Continuous Oversight"[3], to use the four "Human Factors" of friction, uncertainty, fluidity and disorder[4] to his or her advantage, and to maneuver a response that creates a situation with which the adversary cannot cope and his or her will to continue is broken.

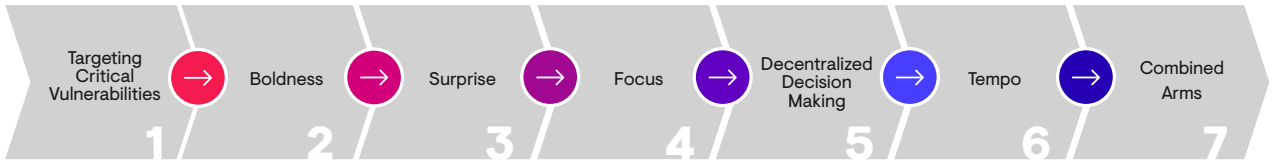
"The essential thing is action. Action has three stages: the decision born of thought, the order or preparation for execution, and the execution itself. All three stages are governed by the will. The will is rooted in character, and for the man of action character is of more critical importance than intellect. Intellect without will is worthless, will without intellect is dangerous."

– Hans von Seeckt, *Thoughts of a Soldier*[2]

Due to the lag in philosophical development toward security, the negative impact of these four factors can be significantly greater if they are not fully addressed in an information security action plan. There are seven maneuver warfare principles that should serve as a foundation for any action plan.

Doctrine of Maneuver Warfare

The "Doctrine of Maneuver Warfare"[5] is based on seven core principles.



The "Doctrine of Maneuver Warfare"

1. Targeting Critical Vulnerabilities

In conventional warfare, the primary focus is targeting critical vulnerabilities that, "if exploited will do the most significant damage to the competitor's ability to resist."[6]

In cybersecurity warfare, the vulnerabilities of the adversary, as well as the attack method being used, can be addressed through threat intelligence. The more significant vulnerabilities to address are those within the unique operational environment of the individual organization and require forward-looking planning and rigorous self-examination.

Rigorous self-examination requires more than an annual vulnerability scan or penetration test, which is too often the norm in information security action plans. The 2017 Thales Threat Report demonstrates how common it is for organizations to fall short when implementing forward-looking planning. Of the 1,100 IT security executives surveyed, 63 percent indicated that their organizations deploy new technologies before implementing appropriate levels of data security.

The speed in which an adversary can act to exploit a vulnerability is dependent upon how quickly an organization identifies and removes it. Due to the rapidly changing threat environment, this can only be achieved with continuous vulnerability scanning in

combination with penetration testing, mimicking the behavior of an adversary, and social engineering training conducted on a quarterly basis at a minimum.

Minimizing the lag time between identification of a critical weakness and implementation of appropriate security controls maximizes the effectiveness of the resources deployed.

Experimenting with various possible threat scenarios will minimize the lag time between the identification and mitigation of targeted vulnerabilities. The tabletop testing of the incident response plan enables the organization to identify, prepare for and practice

response to an attack on critical vulnerabilities instead of predicting a single future event.

Determining an organization's preparedness for particular security scenarios is broken up into three phases.

1. **Scenario Planning:** Scenario planning starts by examining a set of strategic uncertainties, ranking them in terms of the level of likelihood and severity. An enterprise risk analysis, in concert with the most current threat intelligence, could be used to determine values such as liability associated with the scenario should an actual attack occur. High and medium risk-ranked scenarios should be explored with respect to the impact on the operational environment, followed by the development of a response plan. The response plan should be practiced and documented for each scenario.

   An example of such a scenario might be the vulnerability that could be exploited by a self-propagating ransomware worm[7] that, after infecting the first computer, copies and distributes itself to every computer on the organization's network, including possibly business associates.

2. **Scenario Analysis:** Scenario analysis uses intuition, experience, introspection and current threat intelligence to limit the range of variable outcomes in the rapidly changing and disorderly reality of a cyberattack. Organizations should be adopting a top-down, bottom-up approach to targeting vulnerabilities.

   Top-down

   - Think like the adversary
   - Never lose sight of your ultimate objective (i.e., achieving your enterprise security vision)
   - Make extreme demands on resources at the right time for the right reason

   Bottom-up

   - Rely on subordinates
   - Reinforce and reward ingenuity, action and willingness to take a chance
   - Encourage the team members to "speak up" during the formation of the action plan, scenarios and potential courses of action

   Discretion in decision making is always important. Having the conviction to take the advice of team members and make a decision based on that advice, requires the conviction to stand behind that decision in the face of considerable resistance. Test the decision by encouraging team members to disagree and present alternatives that have the potential for a better outcome.

Reinforcement and training in speaking up can be accomplished by devising creative ways to put people in controlled situations of uncertainty, forcing them to make decisions. A perfect opportunity for this exists when performing tabletop exercises with the organization's incident response plan as recommended by the National Institute of Standards and Technology and included in OCR Guidance.

3. **Scenario Execution:** In order to recognize the greatest value from this principle, the security leader must first step outside of the organization and examine every aspect of the people, processes and technology of the business from the perspective of the potential adversary.

   Communications systems must be flexible and reliable to meet the task at hand. Disaster recovery and backup plans must be documented, practiced and continuously improved.

   - Use all available threat intelligence to rehearse the cybersecurity plan and refine the plan in light of potential outcomes that were not anticipated prior to rehearsals.
   - Live and operate by the philosophy of: "A good plan, violently executed now, is better than a perfect plan next week."[9]

   With this understanding, the leader should be visible to the organization. Lead from the front and get information from firsthand observations. Quiz the staff on their responsibilities. Actively seek opinions on decisions from people in the business units regarding their ability to maintain productivity during recovery.

Acknowledge the reality that the adversary is performing a similar reconnaissance of the organization's critical vulnerabilities.

2. Boldness

This principle requires the use of a risk-reward trade-off framework to increase the organization's inclination to make bold decisions, train people to evaluate choices and make decisions, and act in the absence of complete information. In tandem with the calculated risk-reward trade-off of the bold action, there must be a plan for exploiting the opportunity created should the action be successful.

Boldness requires the daring to commit resources to endeavors with highly uncertain outcomes that entail considerable risk. Boldness requires:

- Conviction to stand behind a decision in the face of considerable resistance
- Identification of a breakthrough opportunity and acting decisively to take advantage
- Exhaustive planning to mitigate calculated risks associated with the opportunity in order to create a more favorable risk-reward profile

While boldness is most often associated with taking action, it also includes inaction, abstaining from an uncertain and potentially undesirable situation, keeping in mind that being aggressive may prove to be an unsafe strategy as well. Therein lies the paradox. It is imperative that the leader ask the question, "What is the best strategy to defeat the adversary's strategy for circumventing the controls I have employed in this situation?"

The 80% Rule can be applied to situations that require boldness in the decision-making process. This rule states that "delaying any decision so that it can be made with more than 80% of the necessary information is hesitation."[10] The importance of intuition: There will be times when the tempo[11] of the situation will not permit the exhaustive, meticulous planning and information gathering to mitigate the risks that are associated with a bold decision. In such a situation, the leader must rely on intuition. The training of leaders in preparation and planning during the scenario analyses can help develop keen and quick insight in the face of limited information, enabling the exercising of initiative with confidence. Reinforcing ingenuity, action and willingness to take a chance should be encouraged and rewarded by the security team leader.

BOLDNESS

"Boldness requires calculated risk taking: appropriately weighing risk and reward so that reckless behavior is avoided in the pursuit of breakthrough results."[12] The following relationship formula will serve in calculating risk and reward:

$$\frac{\text{(PROBABILITY OF SUCCESS x POTENTIAL RESULTS FROM SUCCESS)}}{\text{(PROBABILITY OF FAILURE x POTENTIAL COST OF FAILURE)}} - \text{EXPECTED VALUE OF OUTCOME}$$

The inputs require considerable thought and will most often be determined by estimates based on the team's experience. If lacking in that experience, an outside party might be commissioned to assist in determining the input estimates. It's important to weigh the risk and reward, be patient and disciplined in committing resources to a decision, and always consider the question, "What's the downside?"

A final action, associated with this principle, involves documenting the details of past risk-reward decisions, both successes and shortcomings, in order to accelerate development as a calculated risk taker.

Boldness will play a key role in reorienting the focus of information security from compliance to a strategic information security program of which compliance is but one component.

3. Surprise

The purpose of surprise in maneuver warfare is to proactively take steps to degrade the quality of information available to the adversary. The result could be that the adversary is forced to make decisions that may result in exposing his or her presence earlier than planned. "It is not essential that we take the enemy unaware, but only that he becomes aware too late to react effectively."[13]

Stealth, ambiguity and deception are three approaches that can be used to achieve surprise.

Three Approaches for Achieving Surprise

1. **Stealth** denies the adversary any knowledge of an impending action. During a threat hunting engagement, stealth can be effective in covertly detecting the presence of an adversary, which can then be followed by the development and deployment of a response strategy that catches them completely off guard and prohibits an effective reaction.

   The normal response to the detection of an adversary's presence is to immediately shut down the affected systems. However, the better response might be to use stealth to conceal your intentions or coordinate your efforts with members of your Incident Response team. With coordinated effort, your first move will not announce the timing or direction of your initial response. This stealth approach allows organizations to understand the pervasiveness of the threat without alerting the adversary ahead of the response, thus restricting his ability to change the initial strategy of his attack.

2. **Ambiguity** is "acting in such a way that the enemy does not know what to expect." The cybercriminal conducts reconnaissance of a target organization to better plan the strategy and timing of their attack. Creating ambiguity for the adversary can be accomplishedby staggering activities such as vulnerability scans, penetrations tests and threat hunting exercises in an undetectable pattern. In doing so, the adversary must address the risk of detection and alter his strategy to remain undetected.

   By applying stealth and ambiguity, surprise is achieved, and the will of the adversary weakened, if not broken.

3. **Deception** involves misleading the enemy on your plan of action. This is probably the most difficult approach to achieving surprise in cybersecurity warfare. It might be most applicable when responding to a successful breach that has compromised critical data. In that situation, determining if data has been exfiltrated would require actions that could be anticipated by the adversary. Through the futures scenario analyses conducted according to the boldness principle, planned actions could be rehearsed for the purpose of deceiving the adversary and stopping the exfiltration of the data.

4. Focus

In conventional warfare, focus is the generation of superior combat power at a particular time and place. In information security, superior combat power can only be achieved by expanding the focus beyond prevention to include detecting, responding to, and predicting future attacks.

The focus must also extend beyond the compliance-driven protection of customer data. A holistic focus will better enable the organization to shift resources and manage the business risk with the implementation of measures that target the sophisticated adversaries of today and the predicted growth of targeted attacks. This is particularly relevant to the response aspect of a cybersecurity action plan.

The security culture of an organization is what creates unity and aligns every member of the organization. The focus of the effort is critical to success; it requires considerable balance and creativity if it is to be maintained. It also requires the willingness to assume certain risks presented by a situation.

Executive leadership should designate a primary initiative since this will ensure that focus is a formalized process, which will help reduce conflicts associated with the assignment of resources. Commit your most skilled security personnel to frontline leadership roles to directly supervise the application of resources in order to provide the best opportunity to achieve that focus. This often requires placing people in positions outside of their “comfort zones” but will lead to more well-rounded security specialists who will be able to adjust to the continuously changing threat environment.

As the situation changes, the security leader may shift the primary initiative in the direction that offers the greatest success but introduces new risks. This entails training the team to become comfortable with shifting quickly to meet a new situation. This training is an element of “Continuous Oversight” and must be reinforced with regular communication to the team that includes advanced— as early as possible —notice of a pending change.

In all situations, threat intelligence can provide insight to weaknesses associated with a specific attack vector. Knowledge of an opponent’s weaknesses can provide the opportunity to bring strength, in the form of controls, against the attack.

Integrating all available information will help to guide the application of resources and enable a smoother change of focus that is dictated by a change in the threat environment.

Proactive management of the risk associated with a particular focus will improve flexibility when change is required. Communication with your team, as well as the business units affected by the change in focus, will help ease the transition. Before making a change, consider the downside when weighing the risk and the level of effort needed to shift the resources back after the threat has been mitigated.

Developing a high degree of proficiency in focus can help overcome the deficiency in technology, people and funding that so many security teams experience.

5. Decentralized Decision Making

Every individual has the need to feel competent at what they do. There is no better way to satisfy that need than to demonstrate confidence in their decision-making capability by giving them the authority to make decisions in critical situations.

"Never tell people how to do things. Tell them what to do, and they will surprise you with their ingenuity."[14]

In any dynamic and rapidly changing environment such as information security, success is often the result of an immediate action. Decentralized Decision Making relies heavily on an understanding of the security leader's intent and enables those closest to the action to take advantage of on-the-spot information, not immediately available to their superiors and allows them to exercise initiative. The individual who can make and implement decisions consistently faster gains a tremendous, and often decisive, advantage.

In the case of cybersecurity action plans, the trust necessary to reinforce this principle is built during the regular tabletop exercises, testing the incident response plan and the continuous oversight of the daily execution of the plan. By delegating the authority to make these decisions and tailoring communications with the aim of arming the frontline personnel with the "bigger picture" into which their actions fit, they will vigilantly supervise the directives of the action plan.

Distributed authority is, by nature, chaotic and has the potential to add increased chaos to the dynamic and uncertain situation that surrounds a cybersecurity attack. This chaos can result in a higher prevalence of mistakes, especially when an overzealous subordinate fails to act in concert with the security leader's intent. When executing on this principle, the risk-reward trade-off must be accounted for in the action plan. The situations in which such a decision, by an individual, disproportionately determines the outcome of a large-scale competitive encounter also carries considerable risks.

There are three variables that require attention to detail if this principle is to be used successfully.

1. **Trust and open communications must include a clear understanding of the security leader's intent (vision).** Trust is earned through the leader's daily supervision and presence. As a result, communication channels and processes are developed that enable the free flow of communication during the period of stress. The leader is then able to ensure that his intent is being achieved without suppressing the individual's initiative.

2. **The degree to which the subordinate has authority to make decisions will vary by individual.** In best case scenarios, the subordinate has been delegated the full authority to respond in a manner that results in sufficient speed to allow the organization to avoid missing opportunities. By not having to request permission and wait for orders from a higher authority, opportunities will be seized, and the level of potential compromise minimized.

3. **The security leader's intent, while originating from the top, is actually a mutual agreement.** The agreement includes the leader's vision integrated with the actions of the subordinates. Both pieces must be honored by each party and the subordinate must not fear the leader's wrath if he must seek help to avoid a potential disaster.

By addressing these variables, "Decision making thus becomes a time-competitive process, and timeliness of decisions becomes essential to generating tempo."[15] These frontline decisions can mean the difference between experiencing a breach impacting private customer data and requiring notification to regulatory institutions or stopping the infiltration before such action is required.

6. Tempo

Tempo is relative speed in time. War is a series of moves and countermoves in which the tempo of execution is important. The competitor who is able to respond faster than the opponent can identify opportunities and make decisions that force the opponent into a constant state of reaction. The constant state of reaction results in breaking the opponent's will to continue the attack and causes them to redirect to another target. The tempo of today's threat actor continues to increase at a pace that exceeds that of the typical organization. The rapid increase in malware variants that are designed to exploit vulnerabilities of existing infrastructure, new technology and persistent human error or negligence are outpacing the industry's ability to respond.

In addition, the typical organization has other priorities that interrupt or delay tempo, including prioritization of compliance over security. Consequently, the typical organization is not matching the tempo of the threat actor, much less operating at one that impedes the adversary facilitating a competitive situation.

Air Force Colonel John Boyd first introduced the mental process of tempo in his lecture, "The Patterns of Conflict." He identified the four-step mental process of: observation, orientation, decision and action. He theorized that each party to a conflict first observes the situation.

- On the basis of the observation, he orients; that is, he makes an estimate of the situation.

The rapid increase in malware variants that are designed to exploit vulnerabilities of existing infrastructure, new technology and persistent human error or negligence are outpacing the industry's ability to respond.

- On the basis of the orientation, they make a decision. And, finally he implements the decision — he acts.
- Because his action created a new situation, the process begins anew.

Boyd argued that the party that consistently completes the cycle faster gains an advantage that increases with each cycle. His enemy's reactions become increasingly slower by comparison and, therefore, less effective until his will to continue is broken.

In cybersecurity warfare, this process has great merit. If the orientation and decision steps are integrated with threat intelligence, the subsequent action should provide an advantage to the defender relative to the risk-reward trade-off resulting from a bold decision.

Continuous oversight plays an important role in tempo. The principle of tempo is only effective if leadership is regularly visible and stressing the importance of enterprise security as envisioned in the action plan. By leading from the front and pushing decision-making to lower levels, the tempo of a response will increase. Decentralized decision-making eliminates excessive debate, and the maneuver warfare practitioner is able to seize the initiative.

In seizing the initiative, a superior state of preparedness for the countermove and a position of relative advantage are assured, resulting in an enhanced ability to predict and prepare for the adversary's next move.

7. Combined Arms

Combined arms is the integration of complementary weapons in a manner that creates a synergistic effect and places an opponent in an inescapable, hopeless situation, otherwise known as the horns of a dilemma."[17] In information security, this is the integrated deployment of technology, people and processes in a manner that increases the collective effectiveness of the organization's action plan.

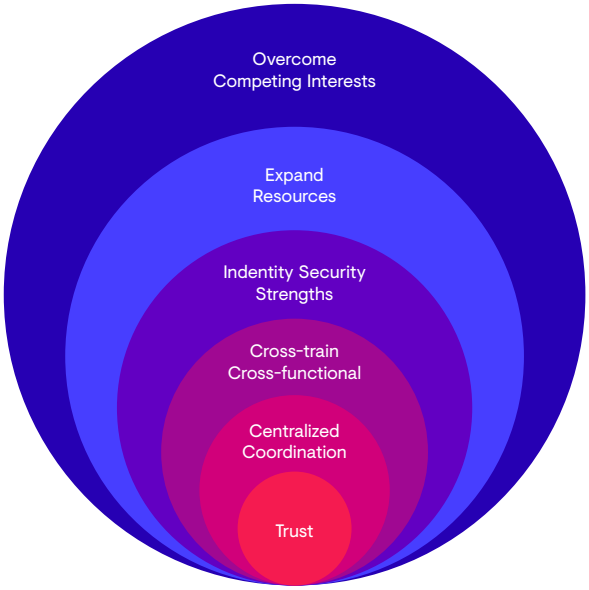
Combined arms can be incredibly effective, but it is an inherently complex and difficult endeavor that demands the utmost cooperation, practice, communication and implicit understanding throughout the organization.

In information security, its effectiveness is dependent on extensive cross-training of the security team member's specialties to instill a better understanding across functional areas of their role in the combined effort.

A key determinant of success in the use of this principle is overcoming competing interests that might exist within the IT department, the information security team and the business departments dependent on both to operate in a manner that enables

"The challenge for every organization is to build a feeling of oneness, of dependence on one another because the question is usually not how well each person works, but how well they work together."[16]

the maneuver warfare practitioner to have a response no matter where the adversary attempts an infiltration, a higher likelihood of success can be expected. This approach requires the utmost trust and coordination throughout the organization and all parties of the Combined Arms team. The team must have one leader to effect centralized coordination and operate and cross-train on standard operating procedures. The result will be a multifaceted, custom-tailored team that operates with improved understanding of the security vision being implemented.



Success requires more trust in functional leaders and their subordinates. Cross-functional cooperation must be rewarded with recognition, compensation or promotion, and there must be a constant reinforcement of the combined arms mindset.

Maneuver Warfare in Summary

The principles for maneuvering in the continuously changing environment are applicable to any situation that requires flexibility and rapid response to that change. Each of these principles can be applied individually but maneuver warfare is about applying these principles simultaneously — in subsets or as an integrated whole — to affect the most decisive and positive outcome at the least cost.

Applied in an integrated manner, the principles complement and reinforce one another. It does not require the leader to become a master tactician, but it does require an increase in bi-directional trust if it is to be executed efficiently.

Maneuver warfare is difficult and requires a high degree of self-confidence, a healthy appetite for calculated risk and an unwavering commitment of the leader and executive team. It requires a radical change in the philosophical approach to security. Security must become a business priority, not an IT issue, and should be "baked into" all business processes.

The Value of Risk Mitigation

The risk to the organization and to the customer is the compromise of the confidentiality, integrity and availability (CIA) of information. Examples of the possible causes of, and ramifications from, the compromise of CIA include:

- The compromise of the confidentiality of information can be caused by snooping on friends, colleagues, neighbors or famous people, with the intent to sell information to the media or post information on social media for revenge or personal gain. The ramifications on the customer can include; identity theft, reputational or relationship damage, employment backlash, financial impact, anxiety and depression.
- The compromise of the integrity of information can result from bad actors stealing credentials for use by family or friends, or hackers to sell on the black market.
- The compromise of availability of information can be caused by incomplete business continuity plans following a ransomware attack.

By applying the Doctrine of Maneuver Warfare for the protection of health information, the likelihood and impact of a cyberattack will be lessened. The due diligence should avoid reputational damage and reduce regulatory fines or legal expenses, in addition to the operational cost and distraction of onerous corrective action plans demanded by regulatory agencies. That work should also provide a strong defense against lawsuits.

The benefit of risk mitigation, indeed the value of risk mitigation, includes:

- Stronger financials for the organization as the result of eliminating or reducing reputational and financial repercussions
- Peace of mind for the executive team, board and engaged employees involved in the protection of customer information
- Increased customer confidence due to the confidentiality, integrity and availability of their information
- Lower career risk — leadership is being called out more and more as being responsible and accountable for protecting this sensitive and personal information

Conclusion

Time is of the essence. The impact of a data breach on an organization can be devastating; the ensuing operational disruption can involve financial, regulatory and brand damage.

By connecting the dots between confidentiality, integrity and availability of information, CFOs and CEOs will see the value of cybersecurity to their organization's brand and customer confidence, which are inextricably linked.

Those who make the investment and maintain the necessary commitment to take this war seriously will succeed in reducing the likelihood and impact of a breach at a significantly higher rate than those who do not.

Sources:

[1] Carbon Black, Carbon Black Threat Report: Non-Malware Attacks and Ransomware Take Center Stage in 2016, December 15, 2016, https://www.carbonblack.com/2016/12/15/carbon-black-threat-report-non-malware-attacks- ransomware-take-center-stage-2016/

[2] Seeckt, Hans von, Thoughts of a Soldier, trans G. Waterhouse (London: Ernest Benn Ltd., 1930) p. 123

[3] At the core of continuous oversight are people regularly reviewing the dynamic threat landscape of the healthcare industry and applying their current knowledge with that threat intelligence to measure the effectiveness, relative to security (i.e., security assessments) against policies and procedures, physical safeguards, network and server security, and application security.

[4] "Justifying Cybersecurity Investment with a Warfare Mindset", SecureWorks and Clearwater Compliance LLC, https://www.secureworks.com/resources/wp-justifying-cybersecurity-investment-with-a-warfare-mindset

[5] "Doctrine is a teaching advanced as the fundamental beliefs of the Marine Corp on the subject of war, from its nature and theory to its preparation and conduct." JCB Pub. 1-02: Doctrine – (DOD, IADB)

[6] Harel, Yehuda, Follow Me: The Story of Moshe Dayan, Olive Books (1972)

[7] Corey Nachreiner, CTO, WatchGuard Technologies

[9] Ibid

[10] Santamaria, Jason, Vincent Martino, and Eric Clemmons, The Marine Corps Way: Using Maneuver Warfare to Lead a Winning Organization, McGraw Hill Books (2004), p. 55

[11] Tempo is often associated with a mental process known variously as the "Decision Cycle of Observe, Orient, Decide, Act" pioneered by Air Force Colonel John Boyd. Also see the Tempo principle explanation later in this paper.

[12] Santamaria, Jason, et al., The Marine Corps Way: Using Maneuver Warfare to Lead a Winning Organization, McGraw Hill Books (2004), p. 57

[13] Warfighting, p. 42

[14] General George S. Patton

[15] Warfighting, p. 89

[16] Vince Lombardi, Head Coach, Green Bay Packers

[17] Santamaria, Jason, et al., The Marine Corps Way: Using Maneuver Warfare to Lead a Winning Organization, McGraw Hill Books (2004), p. 123

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia

Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp