Global Information Assurance Certification Paper

Information Operations:

An Orchestra of Protection

Abstract

This paper will examine the management and protection of information facilitating the decision making process of a security operations team. The team's ability to make decisions that do not compromise security relies on their accurate awareness of the entire information infrastructure. By integrating people, procedures and technology, a framework can be created from where a clear perception of the surrounding environment can be visualized on demand. This will allow the security operations team to gain the upper hand over the threats that an inter-networked community introduces.

John Petropoulos
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
Option 1: Topics in Information Security
October 2004

Table of Contents

Introduction

There is no doubt about it; this is the age of information. Information attack methods have increased in complexity, and no longer is the case that only our information systems are attacked, but also the people behind the systems. Information warfare techniques are being used by attackers in such ways that they can distort our reality, and force us into a reality that they have created for their own benefit. With the advent of cyber terrorism and the increase of security awareness across the world, everyone is looking for an answer to how we protect ourselves from an information attack. Questions are being asked: what needs to be done to counter this threat? How do we protect our privacy? How do we grab a hold of the situation and gain the upper hand? As the old saying goes "You fight fire with fire", thus the security community will need to start using defensive information operations to defend itself against offensive information operations.

Governments and corporations have begun to realize that their information needs to be protected against these multitudes of growing threats. Governments have started passing laws to protect information and hold individuals responsible for not meeting minimum security standards. For instance, Canada's Personal Information Protection and Electronic Documents Act help protect the people's privacy and hold companies responsible for the protection of their client's information (GoC PIPEDA). The private-sector has also increased spending in information security so that they comply with these new laws and prevent disastrous information leakage which can cost the company millions. According to Gartner, Inc, security spending will increase from 3.9 billion dollars in 2003 to 5.8 billion dollars by 2006 (Gartner Dataquest). Robert Lemos, from CNET news.com, reported on a study conducted in 2003 that 62% of senior executives will increase security spending to satisfy legislation (Lemos Legislation Driving…). These trends prove that the information security market is flourishing and organizations are looking for their networks to be secured. This will require that an organization's IT/IS team needs to begin to leverage their monitoring capabilities while maintaining a secure infrastructure.

A security operations team's ability to ensure a secure network is dependant on their awareness of the environment. To get a proper picture of the environment around them, a team needs to be able to deal with the influx of information that allows for a decision-maker to get the pertinent information they need, when they need it. This information influx needs to be gathered and analyzed efficiently while minimizing the time it takes to understand the resulting knowledge which can then be used to make informed decisions that do not adversely affect a company's business goals or security posture.

The solution stems from a much deeper form of thought. Security professionals will have to start looking at how knowledge is created and used in making well thought out and rounded decisions. The way people make decisions needs to be investigated, and understood so that the decision process can be applied quickly in a vast range of situations. To facilitate the decision making process, access to knowledge needs to be available on demand, and the same information needs to be available in the future. To accomplish these goals new methods need to be

developed. In addition to knowledge management, teams will need to be able to communicate over private infrastructure and effectively coordinate activities amongst various teams and partners.

In order to achieve this, a new type of system needs to be created in which a well orchestrated balance of people, procedures and technology, all working in harmony, result in a secure information infrastructure.

Understanding Information

To begin creating a foundation to resolve the information management problem that security professionals are faced with today, an in-depth understanding of information needs to be achieved. This section will help establish an understanding of information and detail several more specific forms of information.

What is Information?

In this third wave of social transformation, information has become a valuable resource, but does anyone really understand what information is? Although many have written about the topic, a clear understanding of what information is cannot be agreed upon. William Martin states that:

> …even the information science profession, whose interest lies in the study of information and related phenomena, is unable to agree upon an operational definition (qtd in networkologist.com).

Thus, if there is not a clear understanding of what information is, then how can we even begin to protect it, never mind take advantage of it? A good starting point in trying to understand information is to discuss Edward Waltz's four characteristics of information (pp 49-50):

1. Information is abstract.
2. Information can have multiple or simultaneous uses.
3. Information is inexhaustible but may perish with time.
4. Information's relationship to utility is complex and non-linear.

Waltz describes abstract information as being an intangible asset that can be a noun or a verb. For instance, a measurement of how long it takes to drive from Calgary to Winnipeg; the specifications of the newest processor in the market and the process for putting together that new IKEA table are all examples of information.

Secondly, this same information can have multiple uses. For example, the processor's specifications can be used by a potential computer buyer for comparative purposes, while the competitor may be trying to determine how well his product can compete in the market.

Waltz's third characteristics of information is that the value of information decreases with time but there are no bounds to the amount of information that can exist. Staying with the examples above, the specifications for the newest processor would be more valuable than the specifications of a processor that is 4 years old. Meanwhile the engineers over at our favorite vendor's lab are coming up with new methods of creating better and more efficient processors.

Waltz's fourth and final description stated that information's relationship to utility is dependant on a variety of factors (pp 50). Information can be quite valuable in one context, but not be as fruitful in another. For instance, a new concrete mix may save New York State DOT millions of dollars, while the same information will

not be as valuable to a telecommunications company (FHWA How Decision Makers Value Information).

With the above description of information, a deeper look can be taken into how information evolves into more valuable forms.

Transformation

Taking a technical approach to defining information reveals that it can exist in three separate states. The first level, which is also the one with the lowest value, is data. Data is the collection of observations or measurements. When data is manipulated and organized it is transitioned to the next state; information. Information will be defined as an organized and manageable set of datum. The final transformation happens when the meaning of the information and all the interdependent relationships between data sets is understood. This type of information is called knowledge and is the most valuable type of information that can exist.

This description of a transformation may seem strange because all three states can be referred to as information even though the second most valuable state is actually called information. To clearly understand this, the word information can encompass all three states of information and when used in a broad context will refer to any or all of the three states. When the word information is used in a more precise and exact context, it usually refers to the state that the information is in. For this text, these rules will be followed.

Figure 1: Knowledge Creation

Making Information Useful

In an environment where information translates to dollars, the process of creating information needs to be streamlined. Joint Publication 3-13 shares this vision by stating "Defending against [Information Operations] … is predicated on how well the intelligence process function…" (pp III-11). The question that arises is how does this happen?

From a high level perspective, a five-stage approach can be taken to acquire and transform data. The five-stages as described by one source are (JP 2-0 pp II-1):

1. Planning and direction
2. Collection
3. Processing and exploitation
4. Analysis and production
5. Dissemination and integration

Planning and Direction:

The process begins with the planning phase where decisions are made on what needs to be collected and what will be done with the information collected. This phase would include development of a course of action, the strategic deployment of sensors, supporting resources and architecture, as well as the data collection directives and contingencies. FM 34-130 goes into great detail explaining the intelligence preparation of the battlefield process and essentially maps out this particular phase. The details will be discussed later on in the in the Planning and Deployment section. This phase approaches the situation analytically so that a decision maker can set objectives that attack critical weaknesses, assess risk and develop an assumption of an opponent's possible reaction to an action (FM 34-130; Waltz pp 145-146).

Collection:

The collection of data can come from a wide range of sensors, where a sensor is considered any source of information. All data that will contribute to the overall achievement of the objective should be securely sent to a central repository for organization and indexing functions to take place. There are four critical factors that contribute to the overall success of the collection process: timeliness, revisit, accuracy and stealth (Waltz pp 119).

Timeliness is the amount of lag between the collection of an event and the warning or alert to be received by the analyst (Waltz pp 119). Revisit is defined as the frequency that a sensor can collect data from its environment (Waltz pp 120). The precision of the collected data and predictions generated from the data sets falls under accuracy and finally, stealth is a measurement of secrecy from which the data can be collected (Waltz pp 120).

In sum, the data collection process relies on the timely and continuous transmission of as much correct data as possible without intruding on the target source. All four of these characteristics would need to be taken into account while planning the deployment of sensors.

Processing and Exploitation

During the processing phase the data collected is manipulated and prepared for further analysis. This process can involve a variety of methods that is dependant on the type of information that is to be processed (JP 2-0 pp II-8; FM 2-0 pp 5-6). For a security analyst working on networks, most information would need to be indexed, sorted, stored and perhaps even correlated before it would be ready for analysis.

Analysis and Production

This stage involves a complete analysis of the information. An analyst would develop an interpretation through logic and reasoning (Waltz pp 115). The analyst would need to take into account all aspects of the environment and several indications, account for their accuracy, and develop a plausible evaluation of a series of events. At this point, an understanding of the situation has been attained, the accuracy of any conclusion can be calculated, the

situation can be visualized, and the information can be reported on (JP 2-0 pp II-8; FM 2-0 5-8).

Dissemination and Integration

Assistant secretary of defense for C4I, Emmett Paige Jr. has described dissemination as the mechanism that allows for information to be assimilated, distributed, and processed according to the recipient's needs (Ensuring Joint Forces Superiority in the Information Age). This involves the creation of visuals, reports, diagrams or customizable interface that permits the decision maker to "see" the scenario and make well thought out decisions (JP 2-0 pp II-13; Waltz pp 116). By putting information in a context that the recipient of that information can understand, a clear representation of the scenario can be achieved quickly, and the recipient can act in a manner that supports the business objective. This allows for tighter integration between teams working towards a single objective, thus unifying the incident response team, network support team or any other team that would need to work side by side.

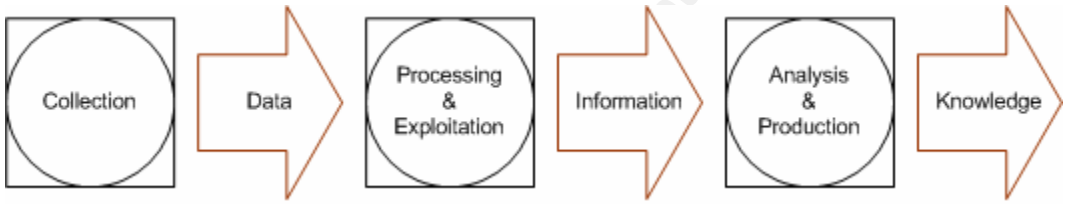

Figure 2: Knowledge Creation Process

Getting into the mind

Before continuing, certain concepts on deductive and inductive reasoning need to be understood.

Understanding decisions through reasoning

Deductive and Inductive Reasoning

Several sources, describe deductive reasoning as going "from the general to the more specific" and describe inductive reasoning as going "from the specific to the more general" (Trochim Research Methods Knowledge Base; Bolton Institute). Basically, deductive reasoning takes a theory and confirms the theory by testing specific data sets. On the other hand, inductive reasoning takes a series of data sets and forms a theory.

The following statement is an example of deductive reasoning:

If you study hard, you will get good grades
You studied hard
You got good grades

This can be further simplified as a logical expression:

A → B
B
∴ A

The following is an example of inductive reasoning:

(2, 4, 6, 8, 10)
All numbers in this set are increasing by two.
Therefore the next number in the set will increase by two.

When these examples are studied closely, certain faults can be found with the logic. Unfortunately, a complete discussion on the subject is beyond the scope of this paper. If a more in-depth explanation is needed, Douglas L. Medin and Brian H. Ross provide an excellent introductory coverage in Cognitive Psychology.

Decision Cycle

The decision cycle discussed here was developed by Col John Boyd, USAF (ret) while studying the reasons of the USAF success during the Korean War. The OODA loop (observe, orient, decide, act) is a decision making process that is used today in the US military services and within the business community (MindSIM Decision Making). It involves a four stage approach that gathers information, analyzes the information, plan development and finally executes the plan. To further support this theory, one can also look at Rasmussen's decision ladder (MindSIM Decision Making). Although Rasmussen's process is quite complex it still displays the overall process of the OODA loop (Davis et al. pp 122). Figure 3 and figure 4 show the decision cycles described above.

This cycle is the hinge to understanding how people, procedures and technology will integrate into a harmonious system. Within the field of information

operations, the OODA loop has been used to attack an opponent's perception of the environment. By cycling through the OODA loop at a quicker pace than the opponent, an attacker can slow down the opponent's decision making process, while protecting and enhancing their own information infrastructure (Lamb pp 62-63;).

This begs the question, if an attacker must manipulate the victims perception, don't they need to get right into their victims OODA loop? Or does the aggressor only need to get into the victims frame of mind?

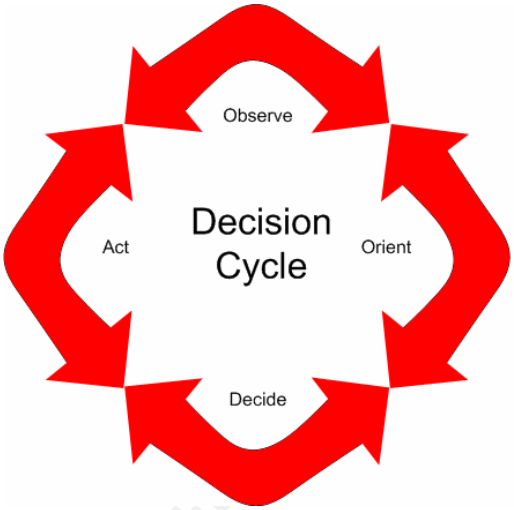

Figure 3: Boyd's OODA Loop

Attacks and the mind

Within the Orient phase of the loop, data evolves into knowledge and decisions are made. Lamb argues that the outcome of future attacks will not be based on getting inside the opponent's OODA loop, but rather the pace and scope of the loop will be the determining factor (Lamb pp 62). Since the cycle itself already incorporates tapping into the opponent's potential course of action, the cycle would only be revisiting the opponent's possible moves quicker. On the other hand, the decision makers would need to foster a dynamic environment, and observe the environment for unthought-of reactions.

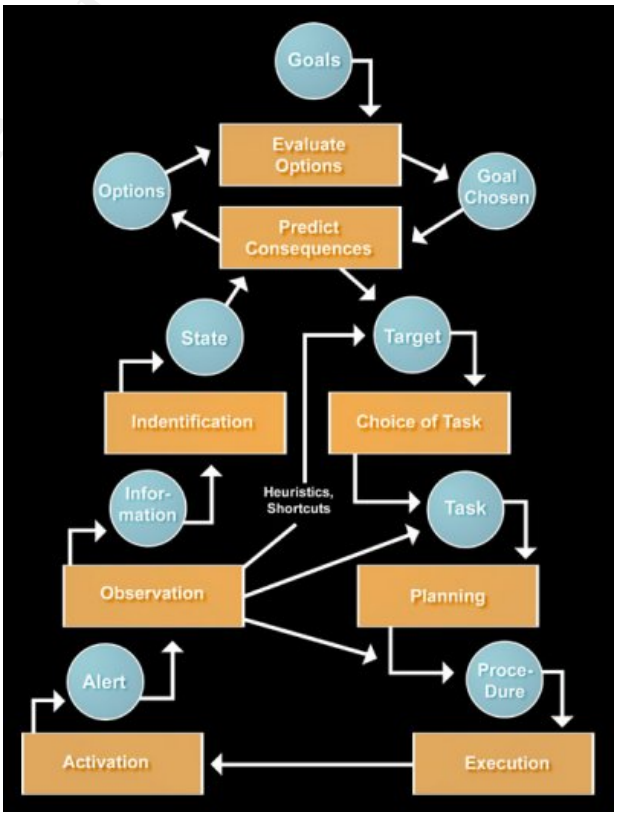

Figure 4: Rassmussen's Decision Ladder. Source: MindSIM

Waltz describes a loop that takes into account three effects of attacks on an opponent; their capacity to act, their perception of reality, and their will to act (pp 4-5). The security professional needs to be made aware of and understand the significance of Lamb's argument of the opponent's OODA loop and Waltz's accounting of attacks to effectively work towards providing a framework that would prevent detrimental negative effects on their own decision cycle. This would involve following security best-practices that cover the protection of all information

resources, from the physical protection of an area, right down to the protection of data. An accurate perception of reality is based on a properly secured environment where sensors are redundant and the environment can be reliably monitored providing cross sensor confirmation. This can bring reaction capabilities and restoration times down to virtually nil and would provide a significant level of security due to an accurate view of the environment.

Achieving an accurate view of the environment requires the collection, processing, and analysis of data, which is more than one analyst can ever handle in a timely fashion. This directly affects the Observe and Orient portion of the OODA loop slowing down the process. This would mean that the knowledge extracted from the data collected would be delivered to decision makers too late, impeding the Observe and Orient phases of the loop, and the opponent would already have the upper hand. The analyst should be able to grasp the situation and develop an understanding that will enhance the decision maker's ability to protect the network. Stephen Northcutt and Judy Novak describe how one of the greatest marketing lies for intrusion detection systems is the concept of "Real-Time" (Northcutt, Novak pp 145). The idea is that all the information is collected at such a great rate that a human cannot possibly be expected to react at that speed (Northcutt, Novak pp 145). This is where technology comes into play.

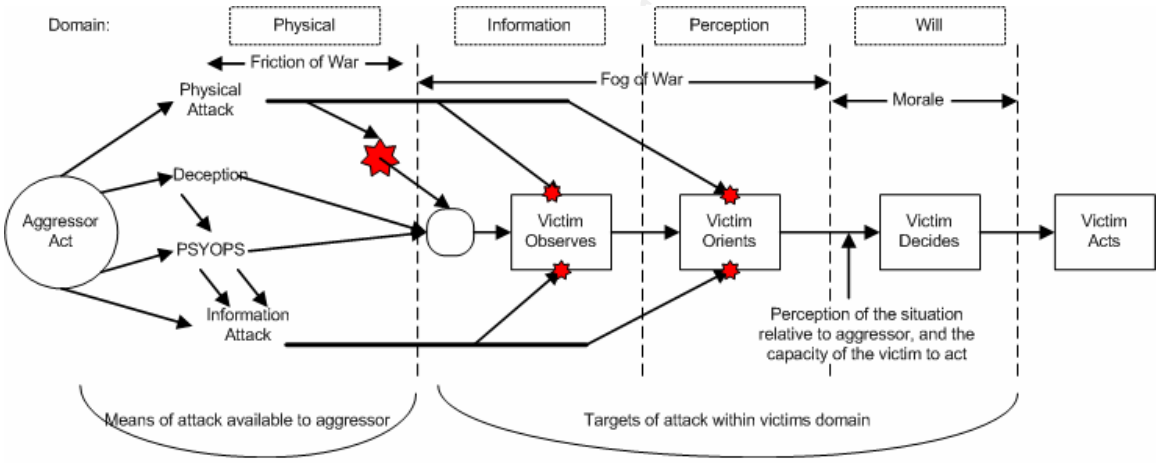

Figure 3: Attacks and the OODA Loop.

Source: Waltz (pp 6)

Technology

A busy network can generate an enormous amount of logs and security analysts need to manage this growing problem of information overload. Decisions should be based on the information that can be confirmed, and on the accuracy of the information that is known. There is nothing like deploying a team of individuals to respond to a low priority threat, while a higher priority incident is occurring somewhere else.

Attacks and countermeasures are gaining complexity and a wide range of solutions are available to security professionals to mitigate risk or contain an attack. The personnel that maintain the network gain valuable experience that is not always or cannot be shared with the company. The sharing of the these experiences help develop the company's security posture by This knowledge management problem needs to be addressed and incorporated into technology leading to a "solution-on-demand" type of architecture.

What we as security professionals should be working towards is a structure where this "solution-on-demand" architecture and information management have been integrated. This framework will need to be interoperable with all technologies and have the capability to grow within an environment that is willing to integrate functions that may support the security information infrastructure.

Waltz describes the role of technology in information operations as the integration of a reactive methodology and proactive methodology processing information within the observation phase of the OODA loop (pp 89). These methodologies are centered on a data fusion and data mining model. The data fusion aspect is responsible for detecting alarms while the data mining piece is responsible for learning new pattern descriptions (Waltz 89-92). In their paper "Why information Explosion can be Bad for Data Mining, and How Data Fusion Provides a Way Out" Peter van der Putten, Joost N. Kok and Amar Gupta, show that these technologies are not only useful in the security field, but also in marketing and other realms. Furthermore, in a Computerworld article by Don Verton, a senior republican congressman, Curt Wekldon (R-Pa), reported that the US government was lacking in a data mining and data fusion model and was quoted "… on September 11th, that [data mining and data fusion] capability did not exist, and we paid the price," suggesting that had there been the capability in place perhaps the attack may have been prevented.

The Joint Forces have already begun looking at interoperability issues and have published their concerns in their Joint Publications. The push to disseminate data over a wide variety of interfaces has grown, and the need for interoperability has become more pressing (JP 2-0 pp II-12-13). Today, protocols and programming languages have been developed to support a wide variety of information dissemination tools that use the infrastructure to relay all types of information, such as text documents, encrypted files, or streaming video.

Information systems that would support the security operations should be up to security standards. Joint Publication 3-13 that states "The protected information environment not only provides the degree of protection commensurate with the

value of its contents, but also ensures the capabilities are in place to respond to a broad range of attacks". Without providing the team with a secure foundation of tools to work with, they would not be able to reliably monitor a network largely because the information that they are working with cannot be trusted. Attackers would be able to capture key systems and create an environment that would benefit the attacker. This idea has been discussed by many but Prof. George J. Stein conveys it best while discussing the impact of television and broadcast news as a tool of information warfare.

> Many people suspect that the national command authorities (NCA) are in danger of becoming increasingly "reactive" to a "fictive" universe created by CNN, its various international competitors, or even a terrorist with a video camera (Johnson). This media-created universe we live in is fictive rather than "fictional" because although what we see on CNN is "true," it is just not the whole, relevant, or contextual truth (Stein Information Warfare).

The example above represents a source of unreliable information because of the fact that the media is only painting part of the picture, distorting the viewer's perception of the actual situation. The lesson learned from this example is: for an accurate situational perception, one must have all the relevant information accessible to them. This is where the collection of information and clear visualization come into play.

Security Information Management

Security Information Management (SIM) tools help control the information overflow problem that security analysts are faced with today. They provide a framework that helps integrate a variety of platforms and automates both the collection and processing phase of the knowledge creation process. Furthermore, they provide an interface for every player interacting with the information space. To achieve this, data that is collected needs to be manipulated into a common format, signatures need to be created, and aggregated data sets need to be investigated to confirm suspicious patterns.

Data Mining and Data Fusion

A proper SIM tool should fit an organization's procedural model. As we shall discuss a later on, analysts will need to react on predefined alerts or analyze data sets to find new patterns and create signatures for those patterns. This is where Waltz's data mining and data fusion model comes into play. Data fusion is the aspect of the tool that contains that alert signatures (Waltz pp 2). It sifts through data and deductively uncovers patterns based on predefined signatures and alerts the user of their existence (Waltz pp 2). To complement this, data mining capabilities help automate the log examination by locating interesting data sets, what Waltz calls abduction, and allows the analyst to inductively determine if the data is related to an event of interest or not (Waltz pp 2). Both technological advances help support the OODA by providing the analyst with reliable visualizations, facilitating the analysis aspect of the Orient phase, all the

while allowing the technology to adapt to an ever changing environment, and enhancing the planning and collection aspect of the Observation phase.

Data Manipulation

SIM vendors, ArcSight and netForensics claim that clients come to them with a variety of problems, where the most prevalent are (Planning and Executing Enterprise Security Management pp 2; Security Information Management pp 6):

- Data overload
- False-positives
- Inefficient incident response
- Incomplete reporting

Both these vendors deal with these issues by "normalizing" the information influx and providing an intuitive visual of the environment. Basically, normalization is the manipulation of log data. As logs are gathered from multiple types of sensors related fields are processed and organized by common fields, and entered into the database, thus facilitating the correlation process (Got Correlation? Not without Normalization). This is done by looking at how the log data is structured for multiple sensor sources and processing the data into common fields. This translates to an event of interest with the investigation logs from several sources hidden within it, saving the security analyst the time to collect, parse and process the logs on every device manually. This function manipulates information and prepares it for analysis as discussed in the Process and Exploitation section of "Making Information Useful" part above. All in all, the normalization of traffic helps achieve a quicker OODA cycle.

The Future

What these technologies do not do today though is keep track of the analyst's availability of a resource. Within the security field, managers and team leaders will need to know when their human, hardware, and software resources are no longer available to deal with incoming issues within a reasonable time-frame to deal with the latest high priority alerts or analyze the latest worm. These service gaps present a vulnerability within the operational aspects of a security service and need to be captured and reported so that managers can react and resolve bottlenecks within the department or build a business case for hiring another analyst or agent.

Taking the same technology to the next level of security response would allow for the monitoring of physical access control systems, area lighting, HVAC systems, fire detection systems, physical intrusion alarms, and even automated video monitoring capabilities. To accomplish this, interoperability issues need to be addressed. The outcome would be a system where complete security awareness will be achievable through a single interface.

Overall, the SIM tool will be the security analyst's hands, feet, eyes, ears and nose in this new age of information protection. This tool will be responsible for gathering and sorting collected information, while looking for anomalies that fall within already pre-established parameters. Furthermore, data will be processed

and prepared for skilled analysts to review and develop more sophisticated entries in the data fusion module. Finally, pertinent information will be delivered to the decision makers through customizable interfaces that enhance the situational comprehension for quicker and more reliable decision making.

Knowledge Management

Knowledge Management tools are used to organize and search for knowledge stored within a database. These tools give the security analyst or any decision maker the ability to retrieve available information the second they need it (Barclay et al What is Knowledge Management). The speed at which this information is retrieved greatly enhances the efficiency of the OODA cycle.

Methods of attacks are getting more and more complicated. It is getting extremely difficult for a single analyst to keep track of all the latest tricks. These knowledge management tools gather all the knowledge of previously worked on cases, or analyst experiences that have been shared through email, and store them into a database, making them available to everyone on demand. The organizational structure allows analysts to search through an enormous amount of data and find solutions to numerous variations of problems (Vogel pp 2-3). Essentially it would be like having the entire team backing the analyst up, even if the team is not available.

The demand for these types of tools is bound to increase. In a survey conducted by Statistics Canada in 2001, it was found that 9 out of 10 businesses surveyed used some sort of knowledge management practice (Statistics Canada pp 9). From these businesses, about 88% of the respondents found that these practices helped improve skills and knowledge while the other 12 percent didn't find the practices that effective (Statistics Canada pp 22). These statistics are clear indications that knowledge management tools are important to an organization's competitive growth.

For the security professional, these knowledge management tools would need to be directly integrated with a SIM tool. When alerts show up on the screen, possible solutions can also appear or at the very least be one click away. If a knowledge management tool and a SIM tool were compatible or integrated, signatures could be created and integrated into the SIM tool for alerting, while at the same time providing the analyst with the knowledge needed to help resolve the alert. This would work similarly to the data fusion and data mining concept discussed earlier (Waltz pp 103-104).

The next logical step to this would be looking at developing automated reaction to functions that could be automated without exposing the infrastructure. Martin Libicki discusses the use of neural nets that learn by experience and create a database of rules from which actions can be taken, but warns his audience on the exposures created by such a system (Libicki). This integration will play a key role in incident management and security enhancement by once again increasing the frequency of the OODA cycle. To attain this goal of automation, the security professional will need to look into integrating change management processes and tools with the SIM and knowledge base tools.

Configuration Management Tools

Configuration Management technologies reduce the cost of device management by automating repetitive functions as well as providing a audit trail for configuration changes and options to revert back to the last known good configuration in case of failures. In a study by Infonetics, Inc., network outages may cost a company as much as 60% loss in revenue (qtd. Cost Analysis… pp 4). In a feature by Suzanne Gasper of Network World Fusion, EDS reported that they expect to save up to 100$ million dollars in operational costs within a three year period due to the deployment of a configuration management tool Opsware (pp. 2) This ties in well with the OODA cycle because the automation of functions and response times in critical situation are important in decreasing the time it takes to act on decisions.

Integration

As discussed in the previous section, tool integration can help leverage the technological interface between human and machine. This is possible by stitching the SIM architecture, knowledge management tools and the configuration management architecture together.

Automating actions based on alerts collected and analyzed through the SIM functions would definitely help create an efficient OODA cycle. Firewalls can automatically be updated across an entire organization, administrators can be notified of critical outages on the network or even automatically download and test security patches. This automation can drastically reduce response times as well as resolution times.

The downside to this type of automation is the existence of false-positives. Automating these functions take time and research. The information collected during the data mining process would need to be studied extensively to create a signature that would reduce these false-alarms. In some cases, not all information may be available and the reliability of the solution to the alert may not be accurate. In those cases, the automation will need to be bypassed, and human intervention will be required.

Interoperability

All managed network devices should be interoperable with the configuration management tool. Having a single tool that can manage all networked devices can decrease training time, decrease maintenance activities and simplify any custom integration. Making such a solution a viable and cost effective management tool. For instance, a tool capable of conducting changes across a multitude of platforms through a uniform interface would reduce the amount of specialized administrators needed to perform the tasks as well as increase the number of devices that can be managed by a single administrator. This would be possible because of the uniform interface. A good example of a situation like this can come from a simple firewall rule change such as adding new services to the DMZ. Such a change would require three to four pieces of information but is done differently depending on the type of firewall or router that is on the perimeter. If this single interface gathered these three to four pieces of

information and complete the tasks, then the administrator entering this data would not need to be an expert in the inner workings of each technology that he has to work with.

Alvin Toffler discusses how the workforce is getting more and more specialized requiring increased training but warns that in every field, organizations are "adding laymen to decision-making bodies"(pp 262; pp 162-168). This can be seen by many in the information security field and has been discussed in newsgroups. On July 26 2004, Don Parker raised his concern about the skill level of some analysts in the field today (Penetration Testing list). The overall consensus was that everybody is seeing the same trend and most of the responders felt strong TCP/IP skills were necessary for a successful career in the security industry (Penetration Testing list). What needs to be taken from this discussion is the determination of the cost of hiring many such specialists.

In the grand scheme of things, hiring a bunch of specialists is not cost effective because of the high salaries involved. For instance, according to Robert Half Technology Information Technology Professionals, a Network Security Administrator in Canada can ask for anywhere between $66,750 to $96,750 (pp 24). Using this information, an organization that needed to hire three specialists to manage the information systems, could cost them anywhere between $200,000 and $300,000 per year! These numbers don't even include any training, benefits or bonuses (pp 2).

The configuration management tool improves the OODA loop by allowing for efficient and cost effective change management. To complement this, proper resources need to allocated to complete specified task and work needs to be coordinated across teams until the functions have been completed.

Enterprise Resource Planning Tools

Although a security team can consist of many individuals with different responsibilities but their job functions are dependant on one another. To facilitate the coordination of resources and tracking of problem scenarios, Enterprise Resource Planning tools can be used. ERP tools are used to track issues until resolution and coordinate resources across multiple teams of individuals.

Tracking

With a larger security team, problem scenarios can be difficult to track from beginning until resolution. An ERP tool can help maintain a record of all incidents or requests as they are occurring, and work notes can be stored.

Carnegie Mellon University/Software Engineering Institute's Handbook for Computer Security Incident Response Teams discusses certain functionalities that a good tracking tool should have. They discuss the need for the tools to support the triage function by providing the ability for incident tracking and prioritization through the issuance of tracking numbers and standard reporting forms (West-Brown, Stikvoort, Kossakowski, Killcrece, Ruefle, Zajicek, Handbook for Computer Incident Response Teams pp 69-74).

The issuance of tracking numbers allows individual stakeholders to easily reference particular case numbers to update information, while the supporting teams can easily find and update the incident work notes as work is being completed. As the case handler updates the incident, standard forms can help the handler follow procedures. Furthermore, a record of the work that was completed can be reported on with incident response time, resolution times or other metrics that can help executives identify bottlenecks and make important decisions about the status of the organization and the teams that run it.

The tracking aspect of ERP tools fits nicely within the Decide and Act steps of the OODA loop. It effectively keeps track of the work and the handlers should not overlap work that was previously done. By doing so, the Decide and Act steps become more efficient and the handling team can move through the decision cycle quite effectively. Additionally, the dissemination of information can be completed through this channel and activities can be coordinated amongst teams.

Coordination

In most circumstances, the issues that arise will need to be coordinated across multiple teams. For instance, a team of individuals responsible for security monitoring will notice an incident, do the initial triage but will have to hand off the issue to an incident response team. To speed up the escalation process, an ERP tool should be capable of alerting individuals of problems that arise, and schedule a resource to perform a job function at a specific hour; this facilitates the coordination issue. The smooth progression from one team to the other greatly enhances the cycle time of the OODA loop.

Using the same example as above, the monitoring team notices and assesses the initial incident. After the monitoring team goes through a triage process, the incident team can be alerted of the incident and queued for the next available handler. As the handler investigates the issue, he can coordinate firewall adjustments, forensic analysis and system restoration through the same interface. These teams are also alerted and their time is scheduled to complete the work at hand.

This tool speeds up the loop by increasing efficiency between when the time decisions are made and actions need to be taken. When the handlers confirm the incident and the need to contain the situation has been established, the decision to create firewall rules or pull the network interface can be communicated to the proper authority and the action can be taken immediately. This realization allows for clean, centralized coordination from desktop to desktop.

Communications and System Support

All information systems supporting the security infrastructure need to be maintained with the highest level of security in mind. The analyst should trust the systems that are processing and reporting on the information collected. Furthermore, redundant and automated fail-over systems should definitely be implemented and protocols should be in place to streamline the analysis hand-off

to a supporting team. Lastly, communication between machines and people should be secure. Communication devices used to contact analysts, managers or executives should support the form of information dissemination they need for quick decision making.

Systems supporting the security information infrastructure should be made redundant and be located in different physical locations where both networks are protected against each other. This will protect the security infrastructure against physical destruction and mitigate the effect of a denial of service attack. To highlight this Dorothy E. Denning describes attacks on the Iraqi command and control infrastructure that involved the destruction of the entire coaxial cable system as well as the electrical power switching system that affected the capability of Iraqi high command (pp 5). An ABC *Nightline* report informed the public that a virus was supposedly installed within a dot-matrix printer that affected mainframe and Windows computers affecting the Iraqi's computing infrastructure (qtd. in Denning pp 5). Attacks such as these either delay or prevent decisions from happening, amplifying the restoration times.

Fail-over protocols should be established so that redundant infrastructures are prepared to take over monitoring and analysis from a compromised sister site. The technological factors that support this network should already be redundant but monitoring capabilities may be split between several geographical locations or set up for a "cold" operational failover. However the architecture is designed, a code of conduct should be established to assess the situation, conduct a damage assessment and report for any missing data or systems that have not failed over for monitoring purposes. This business continuity initiative should be well documented and tested. Shon Harris suggests that the testing be done at least once a year. She describes many testing methods, one of which includes

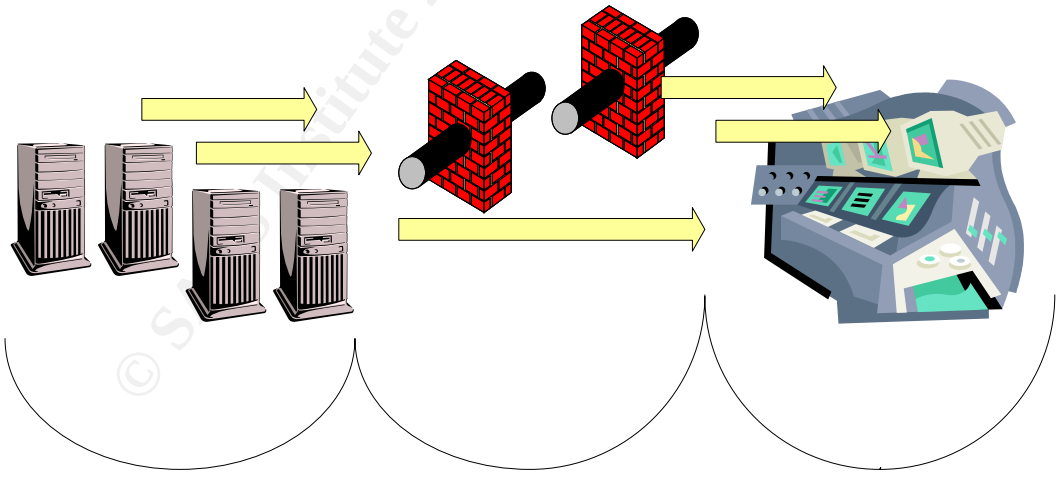

Figure 4: Traffic movement

walking through a predetermined scenario with performance measurements and plan effectiveness measurements (pp 621-624).

Device communication should be authenticated and encrypted to prevent spoofing attempts and eavesdropping attacks. Any device logs or health monitoring capabilities should be protected from end to end. The problem today is that most technologies are not interoperable to provide such functions that leave the communications open for attack somewhere in transit. Simson Garfinkel and Gene Spafford describe a situation where routers are used to protect communication between corporate locations (pp 472-473). The problem there is that once on the LAN the protection provided by the router is no longer useful. Take figure 6 for example, syslog and SNMP are being collected by the monitoring systems and reported against from a firewall device through an encrypted channel. The communications are secured up to the second firewall but are open to eavesdropping and injection attacks from the LAN.

Communication devices that are used to remain in contact with key individuals should be reliable and support visualizations or descriptions used in the decision making process, these devices include, email, cellular telephones, and PDA's. Support for customizable visuals within the SIM and knowledgebase, are useless if the decision maker cannot get access to them when quick decisions are to be made. Joint Publication 3-13 issues directives for a reporting structure that disseminates abnormalities in a timely and continuous fashion (pp III-12). By providing secure communication devices that support the transfer of information needed, the decision maker has the ability to resolve complex situations as well as co-ordinate actions in any time sensitive situation.

Process and People

Technology will only help solve the security issues that we are faced with today, it is the people, and the procedures that they follow, that will need to become adaptable to resolve problems of the future. Gone are the days of strict process flow charts and one-size fits all solutions; adaptation is the name of the game. The future of information assurance rests on our capability to maintain and mold technology, adapting it to the changing environment around us.

Waltz describes an operational concept that would fit a military operational model and maps the operational functions to the OODA cycle while accounting for the flow of information across the physical realm into the information realm and finally the perception (pp 239-242). Figure 7 shows a derivation of Waltz's operational military model that forms the framework between the technologies described in the previous section and the people and procedures described in this section.

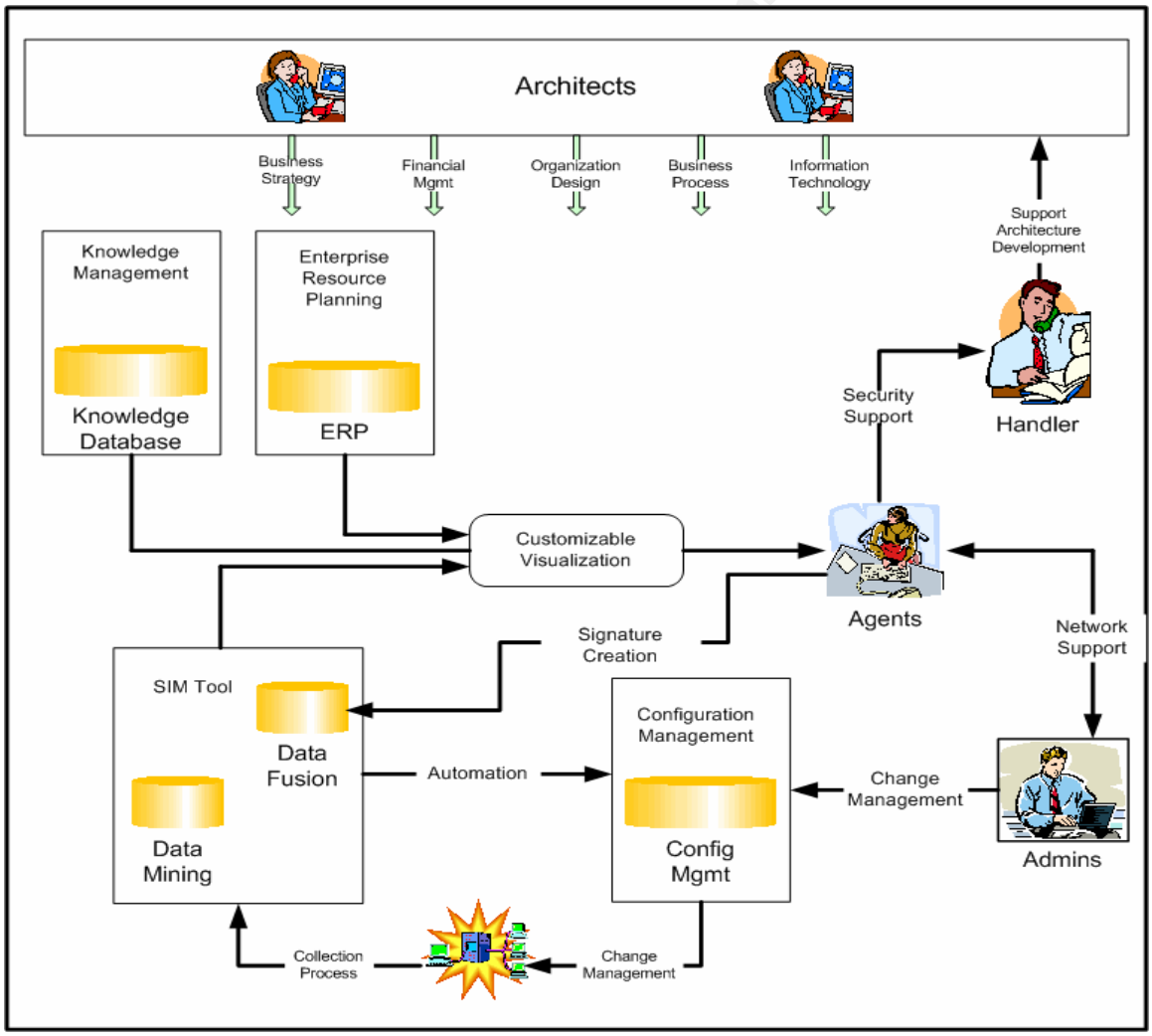

Figure 7: Security Operational Model

In figure 7, the data being collected by the SIM Tool is being analyzed and signatures are being created. As incidents occur, they are correlated with the knowledge management tool as well as the ERP tools and displayed to analysts through a customizable interface and/or an automate response is proactively taken. As the incident is handled, the incident can be coordinated through the ERP tool and any new knowledge created is captured and disseminated through the knowledge management utility.

All security operations can be split into four sections, each supporting the OODA cycle in one form or another. The first, planning and deployment phase involves strategic preparation as described in the "Making Information Useful" section above. Secondly, the monitoring phase includes the security monitoring aspect of security and maps out to the last 4 sections of the "Making Information Useful" section. Thirdly, the device management phase includes maintenance activity and configuration changes for system adaptability; this phase aligns with the Decide and Act phases of the OODA cycle. Lastly, incident handling phase deals with the analysis of security incidents and the procedural integration of any lessons learned from the security incident, that maps out to the Decide and Act phase of the OODA cycle.

All operational activities need to be adaptable and decentralized. Alvin Toffler notices these changes and describes the struggle that organizations were faced with coming into the 80's (pp 230-235). He also forecasts the end of the cookie-cutter solution, and that success lies within what he calls "the fully flex firm" (pp 179-180). What do we, as security professionals, need to do to create an adjustable business structure? Perhaps the answer is in establishing a team oriented approach where all teams act as limbs and interact with one another to produce a viable and flexible solution.

This flexibility will be accomplished by having the incident handlers review incidents and make appropriate changes to the procedure, and technologies. For this to function, the need to maintain relationships that will help preserve the security infrastructure throughout the completion of each phase. This can be fostered by developing programs that allow for the individuals to work across teams. The hardships that each limb faces as they interact between teams will be seen as the individuals work within each aspect of the security operations organization.

Planning and Deployment

The Process

This is where security strategies are developed. The information infrastructure is examined and valuable resources such as databases or web servers are brought in the spotlight. Also, implementation tactics for firewalls, VPN infrastructure, intrusion detection systems and any other security implementation gets mapped out. For this to function, every stakeholder needs to be represented in the decision making process. This will ensure that every team's operational requirements are being met and the development of protocols to call upon other teams, all the while securing the information infrastructure even further.

All teams need to evaluate the network that needs protection. Keeping with the military doctrine, Intelligence Preparations of the Battlefield, a four stage approach can be used. The mapping of the information infrastructure, the effects that come along with the information infrastructure, defining the threats agents, and possible course of action that threat agents may exploit (FM 34-130).

To begin the architect's version of the intelligence preparation of the battlefield, a proper risk analysis is performed. This involves the mapping and documentation of all information resources and their associated risks. Secondly, any issues that are environment specific should be taken into account and plans need to be developed so that they are dealt with accordingly. For instance, laws that pertain to the health care industry may not necessarily be followed by a clothing manufacturer. Thirdly, the threat agents need to be accounted for and possible countermeasures such as firewalls, encryption, and authentication are built into the architecture. Finally, the infrastructure is looked at once again, and possible attack avenues are documented for future reference. This allows for a clean, yet reliable architecture to be developed.

The People

The team responsible for planning and delivering the infrastructure will be the architects. They are the ones that will design the layout of the infrastructure, the procedures that maintain the infrastructure and determine how the information within the infrastructure will be secured. The architects will be going through the Intelligence Preparations of the Battlefield process that includes everything discussed in the section above.

Martin Lamonica, of CNET news.com, describes the job of an enterprise architect in his article Enterprise Architects Clean House: "The job of the enterprise architect is to design a company's computing infrastructure and provide guidelines on how to build and maintain systems" (Lamonica Enterprise Architects Clean House). For the architect to achieve this successfully, they need to have a certain skill set. These architects need to understand the technical and business aspect of the orchestrated system that they will be creating (Lamonica Enterprise Architects Clean House).

The University of California, Irving, list five disciplines that an enterprise architect needs to be proficient in (UCI Enterprise Architect Role):

1. Business Strategy
2. Financial Management
3. Organization Design
4. Business Process Design
5. Information Technology

The first four disciplines involve the understanding of the business aspect of the solution to be designed. The architecture team will need to be able to market themselves and show the stakeholders that investment in such designs will allow them to gain competitive advantage (UCI Enterprise Architect Role). They also need to be able to design the organizational structure and the business process

that this organization will be following, facilitating the integration of the new system into the organization (UCI Enterprise Architect Role). After the business aspect of the architecture has been taken care of, technologies need to be adapted to the business model.

The final discipline, Information Technology, involves technical challenges that the architecture team will be dealing with. These issues involve the designing of the physical infrastructure, the mapping of information flows, application integration and the security of the planned infrastructure from the application layer to the physical layer. The accomplishment of this rests on the technical ability of the team and the skills that each individual will be bringing to the table. According to the University of California, Irving, the architects need to understand all aspects of information technology at a thorough cross disciplinary level (UCI Enterprise Architect Role). Examples of the knowledge that the architecture team will bring to the table include: data warehousing, network design, cryptography, and hardware designing. The successful completion of these tasks set the stage for each function of the security operations team.

Monitoring and Analysis

The Process

The monitoring procedures are designed to observe the security of the information infrastructures. This is where all indications and warnings are analyzed for anomalies that would adversely affect the environment. Device health is monitored to capture possible hardware failures or systems that can no longer handle the load that is being put on them. The sensor logs are being processed and compared to predefined patterns and irregularities, as discussed in the “Data Mining and Data Fusion” section, in search for signs of intrusion or other activity that needs attention.

This is where the SIM tool speeds the process up. Alerts are generated when activity that resembles an attack or imminent failure is occurring on the network. What would normally take hundreds of analysts to sift through is done in seconds. When alerts are captured they are put into perspective by an individual following predefined process, decisions are made and actions are taken, completing the OODA cycle. The actions the are to be taken will be brought to the analyst’s attention through the knowledge management tool and SIM tool integration.

Alerts are not limited to predefined attack patterns. This is where the data mining aspect of the SIM tool captures statistical anomalies and potential relationships between activities that need to be investigated further (Waltz pp 2). The outcome of the investigation process will be documented in the knowledge management tools and initiate a process where new patterns are defined and implemented. This is where skilled analysts gather data sets and inductively reason to establish sound theories for the creation of signatures. This process allows the operational functions to adapt to any environment further enhancing the OODA cycle.

The People

The people responsible for monitoring and analysis work within the Orient and Decide functions of the OODA loop. They are responsible for analyzing and making decisions about the situation. The task of this team of first responders is to receive alerts and develop a coherent perception of the situation. Once that has been achieved, a decision is made to either go through a change management process or to an incident handling process.

The skills involved in completing the tasks above require two sets of analysts. The first being an analyst that is able to take information from the SIM tool and troubleshoot a problem until resolution. This type of troubleshooting requires that the user look at the symptoms, which is information about the problem, and develop certain theories about the origin of the problem to start dismissing the possibilities through deductive reasoning. For example, if a user is having trouble connecting to the network, a good troubleshooter would work up possible theories and test for their existence. They would first verify the physical layer, by verifying the cable, verifying the TCP/IP stack, the network connectivity, and so on. Completing these tasks efficiently require good problem solving skills as well as a technical understanding of the tools and components that the analyst will be exposed to.

The second type of analyst is one that is capable of taking a set of data from the SIM tool to develop new signatures or dismiss the data as normal activity. This is a much more difficult task that requires the analyst to take what he already knows and apply it in different ways to come up with new theories. In Jack: The Jack Of All Trades Security Testing Training Supplement, Pete Herzog developed a training method that got his new-hires thinking out of the box. He states that applied security is based on critical thinking, observations and analysis (Herzog Jack). These skills are essential in maintaining up to date signatures within the data fusion aspect of the SIM tool.

As these analyst solve problems and develop new signatures, decisions will be made and inevitably changes to the infrastructure will need to be made. These changes will require proper testing and management to ensure the successful completion of the OODA loop.

Device Management

The Process

The management section deals with all aspects of the infrastructure that need to be maintained. These maintenance activities include patch management procedures, configuration management duties and the testing of all network changes prior to implementation. These procedures should be clearly defined and followed by the personnel responsible for the infrastructure.

Don Jones, author of Enterprise Network Configuration and Change Management divides the process into six steps (Jones pp 29):

1. Reviewing and approving proposed changes
2. Prioritizing changes

3. Assigning and accounting for risk
4. Monitoring pending changes
5. Documenting and archiving changes
6. Restoring stability after change

Every step within this model helps maintain control in case of changes that do not work well. Every step is also very time consuming, and really slows down the Act phase of the OODA loop. Once the defined procedures have been put in place, the configuration management tool needs to be manipulated to facilitate the process while maintaining control and minimizing risk.

The management team will also need to deal with the other teams within security operations. They will need to support both the monitoring and analysis team as well as the incident handling team. by conducting all change management activities requested by them. Since the device management team is a specialized team, they will also serve as an escalation point for advice on complex network and system issues. This allows for the efficient resolution of technical problems even if they are beyond the reach of the other teams while enhancing the Orient and Decide phases of the cycle.

The People

The type of role that the management team will play corresponds to a system or network administrator role. Every member of the team will need to be highly technical and specialized, possess verifiable problem solving skills and strong interpersonal skills.

As system and network administrators, this team will be responsible for the efficiency of the Act phase of the OODA loop. The technical skills that this team brings forward, coupled with accurate information of the environment that they will be working with, will translate to a clear perception of the effect that a change will bring about.

Incident Handling

The Process

Incident handling, as described by CMU/SEI Handbook for Computer Incident Response Teams, should include reactive, proactive or security quality management services (pp 24-25). This incident handling team will have to offer services that fall within all three realms. The reactive services offered will support the monitoring and analysis team. The proactive services will be supporting the architecture team. The security quality management services will be supporting the policy and procedures as well as the training and awareness programs within the organization.

As the monitoring and analysis team try to deal with the incidents, they will come across a situation where they will need advanced support. The handlers will be able to provide this advanced support, whether the monitoring and analysis team needs simple advice or need to escalate the entire incident to a stronger

capability. What will make the handling team a stronger capability will be their ability to conduct forensic analysis and artifact handling (West-Brown pp26-29).

According to West-Brown et al. the forensic analysis capability is:

> …the collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise (pp 26)

West-Brown's description above has a much deeper meaning which defines the purpose of the handlers. "…to determine changes to the system and assist in the reconstruction of events leading to the compromise", why would the handlers need to take the time to do this? What is the purpose? Taking this in the context of the OODA loop, the knowledge that is acquired by reconstructing the events will lead to quicker cycles, and as Lamb describes, success is based on quicker cycles. The knowledge acquired will help modify procedures, and the security infrastructure to enhance the security posture. Furthermore, the dissemination of the knowledge acquired across the entire security operations team will help shape an accurate perspective of future situations that security operations will be handling.

The handler's will also be working closely with the architects. The handlers will be providing technical support with risk analysis studies, and security audits. While the architects are going through their own version of intelligence preparation of the battlefield the handlers will play a key role in conducting the security analysis. After decisions have been made and the architects solutions have been put in place, the handlers will also have to review and perform security audits on the new services to minimize and document the potential exposures to the system. All these precautions are needed to enhance the decision cycle.

The work that the handlers touch affect all aspects of the loop. When dealing with the architects they will be working to enhance the observation phase of the cycle. When supporting the monitoring and analysis team they are working towards enhancing the Orient and Decide function of the cycle. Lastly, when conducting incident forensic support they are working at enhancing the entire loop for possible future incidents by including adjustments in procedures, dealing with vulnerability to the system and disseminating the knowledge that has been acquired to enhance situational awareness and proactively propose change to the technical aspect of the environment.

The People

CERT/CC released a great document on the basic skills that handlers should have. These skills have been broken up into two categories, personal skills and technical skills (CERT/CC Staffing your Computer Incident Response Team).

According to CERT/CC, the personal skills needed range from skills that can be taught, to the handlers values and work ethic (Staffing your…). The handlers will be responsible for collecting and presenting their findings to their superiors and in some cases within a court of law. Such responsibility requires that the team

members have qualities such as the respect for authority, communication skills, trust, stress management and good ethics (CERT/CC Staffing your ...). These skills define the type of character that is needed to conduct an investigation fairly and efficiently all the while maintaining their composure.

Handlers will be faced with a myriad of security incidents that will involve a clear understanding of the computer networks and computer systems and will need to follow technical procedures to extract information from those systems. The technical skills required to efficiently complete the responsibilities of the handler involve knowledge about security principles, attack methods and counter-attack tactic, and incident handling best practices (CERT/CC Staffing your…). These skills allow for the handler to competently complete an investigation and accurately reconstruct the events leading up to the incident.

The skills that the handling team bring into security operations enhance the OODA loop by providing a support function throughout the loop. During the Observation phase, the team is assisting the architects in painting a clear perspective of the environment. During the Orient and Decide phase, they are providing assistance with the analysis of incidents. Lastly, During the Decide phase of the loop they provide feedback about the root cause of an incident and suggest a course of action to be implemented during the Act phase, thus further strengthening the infrastructure. As security operations loop through the cycle, it is certain that the handlers will be involved in one way or the other.

Training

Every problem that security operations faces will be different from the next. Documented policies and procedures will need to offer direction as opposed to strict guidelines. The people in the frontlines should be able to make well educated decisions based on the information provided to them and the organization's vision. Kevin Mitnick explains that his success in compromising an organization's security was due to the willingness of people to bypass procedures and policy. He goes on to explain that training and education that will mitigate the threat of a compromise (qtd. Security Awareness Toolbox).

Each individual will need training that will allow him or her to understand what decisions they can make and which they cannot make. The training should include a detailed security strategy program, procedural and policy review and. a technology overview

The security strategy program should involve a detailed explanation of threats and countermeasures that the staff member will be dealing with. This training should be conducted in a controlled environment that replicates the employee's working conditions. Security strategies should be discussed and simulation exercises are a necessity to achieving an understanding of the issues that they will be faced with. This will give the analyst hands on experience needed to correctly analyze alerts and inductively develop accurate perspectives. This maps out directly to the Orient aspect of the loop, specifically the analysis and production phase of the knowledge creation process.

The procedural and policy review includes a briefing of the job functions that the staff member will be providing as well as an assessment of the organization's values and expectations. The staff member should be introduced to the job functions through a mixture of on-the-job training initiatives and a formal classroom setup. By integrating both types of training methods, the staff member will be able to apply the skills learned in the classroom, right into the workplace all the while under the supervision of an experienced co-worker. The understanding of the people, environment and corporate values gained at this stage of the training process encourage and develop the Decide phase of the loop by showing the individual who needs to be notified, the types of decisions they can and cannot make, as well as the tasks that they will be faced with on a daily basis.

Finally, the technology overview should cover all technologies that the staff member will need to deal with. This training is best done through a lab setting where configurations can be toyed with and numerous situations can be simulated. For the trainee to be properly prepared for what they will be faced with in real life scenario, they will need to focus on conducting simulations of the daily activities that they will be faced with. For instance, a trainee preparing to join the device management team will need to work with entire networks, building them and configuring them from the ground up. On the other hand, a trainee looking to join the monitoring and analysis team will need to be proficient in gathering information and troubleshooting both network and security issues.

As a follow-up to the training described above, comprehension of the security training, the procedures and policies review should be inspected through testing and process audit, and if need be, corrected.

All aspects of the training process should help increase the OODA cycle by providing the worker with the key principles that they will be applying while on the job. Furthermore, by providing the employee with the knowledge they need to make better decisions, they can quickly adapt to the environment around them and make reasonable decisions, while maintaining the principles of the operation.

Conclusion

The possibility of creating an architecture that allows the analyst to accurately visualize the state of the infrastructure is within our reach. The key to creating this security infrastructure does not lie within a single technological advancement or any set of policies or procedures created by man. It is up to our security officers and their teams to develop a well orchestrated environment that incorporates our natural human behaviors of decision making, reasoning and perception into a system of process and facilitating technologies.

The knowledge to create such a system is out there today. We need to begin looking into the diverse fields of philosophy, psychology, military sciences and cognition to find the perfect systems that are being used today. We have seen how military science and cognition can be brought into the world of network security, yet these concepts are seldom used today.

As we have previously discussed, even governments are neglecting the use of these advancements as reported by Dan Verton in "Congressman Says Data Mining Could have Prevented 9-11". We can also see other governmental agencies suffer from the lack of efficient data analysis. The History Channel's History Undercover also reported that the NSA has been trying to deal with information overload since cellular phones and the internet have become popular in their documentary "Echelon The Most Secret Spy System".

Throughout this paper we have discussed how technologies and people interact through defined procedures to efficiently loop through Col John Boyd, USAF (ret) decision cycle. Each technology helps increase the speed of the loop by assisting its human interface in achieving a goal. As we previously saw, configuration management tools help decrease the Act time by completing management tasks automatically, consequently cycling through the decision cycle at a quicker pace.

Bruce Schneier sums the future of security up best:

> The Coming Third Wave of Internet Attacks: The first wave of attacks targeted the physical electronics. The second wave - syntactic attacks - targets the network's operating logic. The coming third wave of attacks - semantic attacks - will target data and it's meaning. This includes fake press releases, false rumors, manipulated databases. The most severe semantic attacks will be against automatic systems, such as intelligent agents, remote-control devices, etc., that rigidly accept input and have limited ability to evaluate. Semantic attacks are much harder to defend against because they target meaning rather than software flaws. They play on security flaws in people, not in systems. Always remember: amateurs hack systems, professionals hack people.

This just comes to show us how attacks have progressed and security professionals will need to embrace the lessons of other scientific fields to protect our infrastructure better than it is today.

Works Cited

2004 Salary Guide. Menlo Park: Robert Half Track Technology, Information Technology Professionals, 2004

Barclay, Rebecca O., and Philip Murray. What is Knowledge Management. 1997 http://www.media-access.com/whatis.html

Cost Analysis Using CiscoWorks LAN Management Solution. San Jose: Cisco Systems Inc. 2004, http://www.cisco.com/en/US/products/sw/cscowork/ps2425/products_white_paper09186a00800a1988.shtml

Davis, Stuart D., and Amy R. Pritchett, "Alerting System Assertiveness Knowledge and Over-Reliance". Journal of Information Technology, Georgia: Georgia Institute of Technology, 1999, http://www.jiti.com/v1n3/davis.pdf

Decision Making. MindSIM, 2000 http://www.mindsim.com/MindSim/Corporate/OODA.html

Deduction. Bolton England: Bolton Institute Department of Psychology http://www.biology.bolton.ac.uk/ltl/PMG/ded_reasoning.htm

Denning Dorothy E., Information Warfare and Security. Reading: Addison Wesley Longman,1999

DeRodeff, Colby. Got Correlation? Not without Normalization. ArcSight: Cupertino, 2002

Enterprise Architect Role. Irving: University of California, Irving, 2001 http://apps.adcom.uci.edu/EnterpriseArch/EARole.html

FM 2-0 Intelligence, 2004 http://www.fas.org/irp/doddir/army/fm2-0.pdf

FM 34-130 Intelligence Preparations of the Battlefield, Stamford: Corporate Headquarters,1994 Stamford: Corporate Headquarters, http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/34-130/Ch1.htm#s1

Garfinkel, Simson, Gene Spafford Practical UNIX & Internet Security, Sebastopol: O'Reilly, 1996

Gartner Dataquest, "Security Software, All: Worldwide Forecast, All OS Platforms, New License Revenue" 2003 http://www4.gartner.com/media_relations/asset_61940_1595.jsp

Gasper, Suzanne, "Server Savings", NetworkWorldFusion. 2003, http://www.nwfusion.com/research/2003/0331serversave.html?page=2

Government of Canada, Personal Information Protection and Electronic Documents Act. Ottawa:, 2004 http://www.parl.gc.ca/PDF/36/2/parlbus/chambus/house/bills/government/C-6_4.pdf

Harris, Shon, All In One CISSP Certification Exam Guide, Berkeley: McGraw-Hill/Osborne, 2002

Herzog, Peter. Jack: The Jack Of All Trades Security Testing Training Supplement. Institute for Security and Open Methodologies, 2004 http://www.isecom.org/projects/jack.shtml

History Undercover: Echelon The Most Secret Spy System. CBS News Productions 2003, Videocassette. The History Channel, 2004

How Decision Makers Value Information. US:FHWA, US Departement of Transportation 1999, http://www.fhwa.dot.gov/reports/viisvlif.htm

Induction. Bolton England: Bolton Institute Department of Psychology http://www.biology.bolton.ac.uk/ltl/PMG/ind_resoning.htm

Johnson, Douglas V., The Impact of the Media on National Security Decision Making. Carlisle Barracks: Strategic Studies Institute, US Army College, 1994

Jones, Don. The Definitive Guide™ To Enterprise Network Configuration and Change Management. realtimepublishers.com, 2003 http://www.voyence.com/images/ebook/DGENCCM-Ch2a.pdf

JP 2-0 Doctrine for Intelligence Support to Joint Operations, 2000 http://www.dtic.mil/doctrine/jel/new_pubs/jp2_0.pdf

http://www.cdmha.org/toolkit/cdmha-rltk/PUBLICATIONS/jp2_0.pdf

JP 3-13 Joint Doctrine for Information Operations, 1998 http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

Lamb, Michael W. Sr. Bytes: Weapons of Mass Disruption. Air War College Air University, 2002 http://www.au.af.mil/au/awc/awcgate/awc/lamb.pdf

Lamonica, Martin. “Enterprise Architects Clean House”. CNET News.com, 2004 http://zdnet.com.com/2100-1104_2-5278754.html

Lemos, Robert, ”Study: Regulations driving security spending”. CNET News.com. 2003 , http://zdnet.com.com/2100-1105_2-5083758.html?tag=zdnnfd.main

Libicki, Martin. The Future of Information Security. Institute for National Strategic Studies,1998, http://www.fas.org/irp/threat/cyber/docs/infosec.htm

Martin, William J., "The Information Society", Aslib, 1988, http://www.networkologist.com/RapidKnowledge.html

McMillan, Bill. What is Information? http://starform.infj.ulst.ac.uk/billsweb/PGDiploma/InfoSys/1whatisinfo.html

Medin, Douglas L., and Brian H. Ross, Cognitive Psychology 2nd Edition. Troy: Harcourt Brace, 1997

Northcutt, Stephen, and Judy Novak, Network Intrusion Detection, An Analyst Handbook 2nd edition. Indianapolis: New Riders, 2001

Paige, Emmett Jr. Ensuring Joint Force Superiority in the information Age. Norfolk: Armed Forces Staff College, 1996 http://www.defenselink.mil/speeches/1996/di1182.html

Parker, Don, “TCP/IP Skills”, Bugtrack: Penetration Testing List, 2004 http://www.securityfocus.com/archive/101/2004-07-02/2004-07-08/0

Planning and Executing Enterprise Security Management. Arcsight: Cupertino 2002

Putten, Peter van der, Joost N. Kok, and Amar Gupta, Why the information Explosion can be bad for Data Mining and How Data Fusion Provides a Way Out. http://www.crm2day.com/library/EpyVyEkEklPfhGTbEj.php

Security Awareness Toolbox, Information Warfare Site, http://www.iwar.org.uk/comsec/resources/sa-tools/index.htm

Security Information Management. Edison: netForensics, 2004

Schneier, Bruce. Secrets and Lies, Canada: John Wiley & Sons Canada, Ltd, 2004

Statistics Canada, Are we Managing our Knowledge? 2001 http://www.statcan.ca/english/research/88F0006XIE/88F0006XIE2002006.pdf

Staffing your Computer Incident Response Team – What Basic Skills are Needed?, Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003 http://www.cert.org/csirts/csirt-staffing.html

Stein, Prof. George J., “Information Warfare”. Airpower Journal, Maxwell: Air War College, Spring 1995 http://www.airpower.maxwell.af.mil/airchronicles/apj/stein.html

Toffler, Alvin. The Third Wave. New York: Bantam, 1980

- - -. Power Shift. New York: Bantam,1991

Trochim, William M.K., Deduction and Induction, Cornell University, 2004 http://www.socialresearchmethods.net/kb/dedind.htm

VOA News, “CIA Held Back Intelligence on Iraqi Weapons”. New York Times 2004 http://www.iwar.org.uk/news-archive/2004/07-06.htm

Waltz, Edward L., Information Understanding: Integrating Data Fusion and Data Mining Processes. Ann Arbor: ERIM International, 1998 http://ingengineering.com/Documents/Docs-DataFusion/MPA11_6.PDF

- - -. Information Warfare: Principles and Operations. Norwood: Artech House, 1998

West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. Handbook for Computer Security Incident Response Teams (CSIRTs) (CMU/SEI-98-HB-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003 http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb002.pdf

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS